COMMUNICATION ÉLECTRONIQUE & TÉLÉCOMMUNICATION

SEPTEMBRE 2022

WWW.BLOCKCHAINFORGOOD.FR

BLOCKCHAIN @POLYTECHNIQUE
bpifrance SERVIR L'AVENIR
Caisse des Dépôts GROUPE
INSTITUT Louis Bachelier
PB PositiveBlockchain.io

A PROPOS

BLOCKCHAIN FOR GOOD

Écosystème, *Blockchain for Good* est une association de fait depuis 2018 et une association de loi 1901 depuis 2021. Elle a pour objet de valoriser, promouvoir, soutenir et contribuer à la recherche fondamentale et appliquée en matière d'innovations numériques, favoriser et accompagner le partage d'expériences entre l'écosystème des blockchains et les acteurs du développement durable, et promouvoir un cadre législatif et normatif favorable à l'innovation.

NOS PARTENAIRES

BLOCKCHAIN @POLYTECHNIQUE

La **chaire Blockchain@X de l'École Polytechnique** a pour vocation d'allier excellence académique avec prestige institutionnel et scientifique afin de favoriser l'innovation en matière de blockchain. Pionnière dans son domaine et soutenue par Capgemini, Nomadic Labs et la Caisse des Dépôts, elle rassemble des scientifiques en informatique et en économie dont les recherches portent sur les blockchains et les technologies associées. La chaire propose également une offre variée de cours aux étudiants de l'École Polytechnique désireux de s'initier à ce domaine en mutation constante, et contribue à l'organisation de conférences académiques internationales telles que Tokenomics ou Future.s Of Money (FOMPARIS).

Caisse des Dépôts GROUPE

La Caisse des Dépôts et ses filiales constituent un Groupe public, Investisseur de long terme au service de l'intérêt général et du développement durable des territoires. La Blockchain est un enjeu stratégique majeur pour la Caisse des Dépôts, ses métiers et ses clients. Créé en 2015, le Programme Blockchain & Cryptoactifs identifie et implémente des cas d'usages à valeur ajoutée, dans le cadre de projets industriels (Archipels, Liquidshare) ou de partenariats (LaBChain, IRT SystemX), au service du Groupe Caisse des Dépôts et en soutien de l'écosystème, accompagne les acteurs publics dans le déploiement de ces technologies, et contribue aux débats réglementaires pour construire un cadre adapté, au service des enjeux de souveraineté français et européens.

L'**Institut Louis Bachelier** (ILB) est une association de loi 1901, créé en 2008, sous l'impulsion de la Direction Générale du Trésor et de la Caisse des Dépôts et Consignations. L'ADN du Groupe Louis Bachelier (ILB, FdR, IEF) est la recherche scientifique, qui favorise le développement durable en Économie et Finance. Actuellement plus de 60 programmes sont hébergés à l'ILB, avec un focus sur quatre transitions sociétales : environnementale, digitale, démographique et financière. Les activités visent à engager des académiques, des entreprises et des pouvoirs publics dans des programmes de recherche ainsi que dans les manifestations scientifiques et autres forums d'échange.

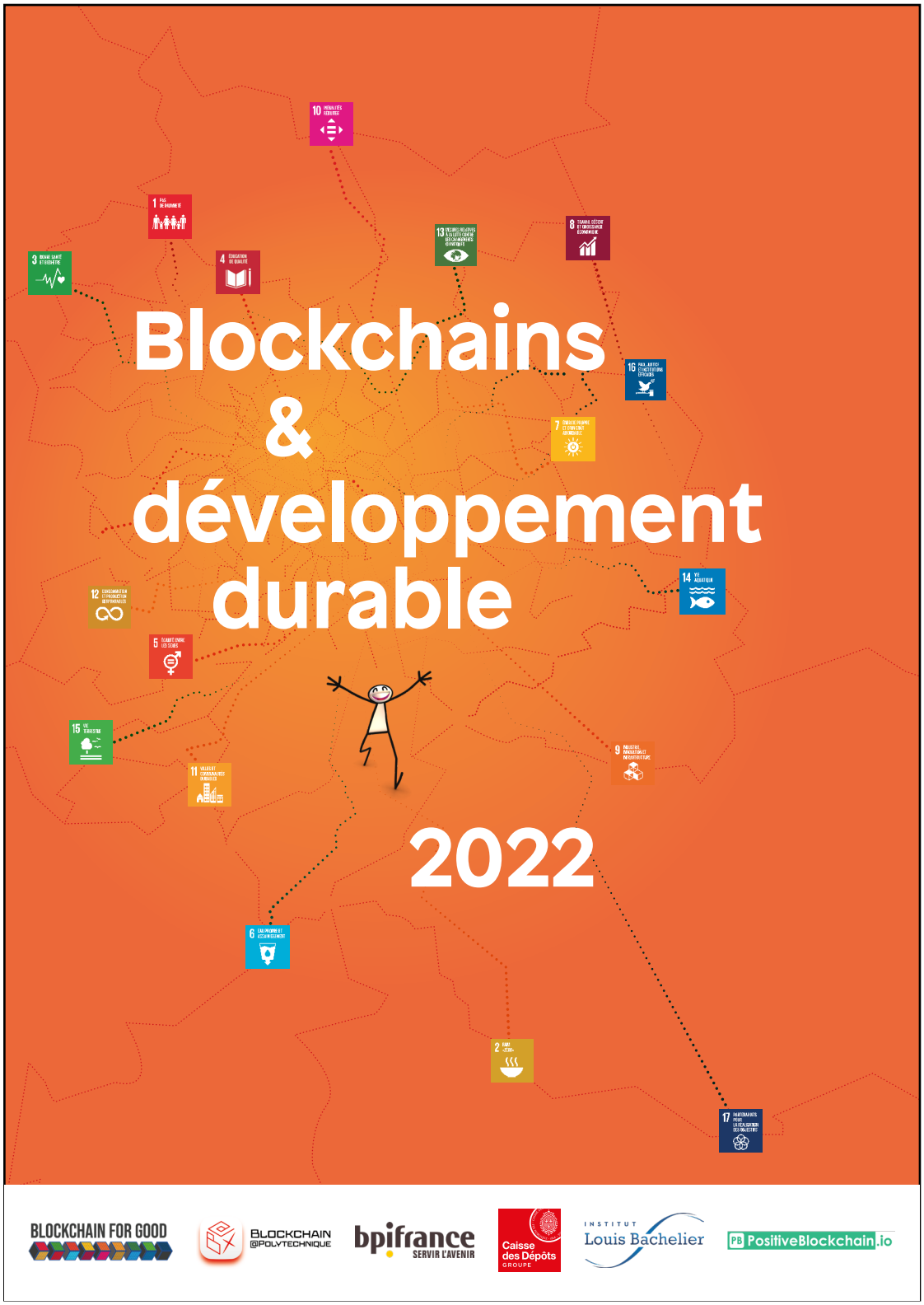
Bpifrance finance les entreprises - à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi leur activité export à travers une large gamme de produits. Conseil, université, mise en réseau et programme d'accélération à destination des startups, des PME et des ETI font également partie de l'offre proposée aux entrepreneurs.

PositiveBlockchain.io est tout à la fois une base de données ouverte, un média et une communauté qui explore le potentiel des technologies blockchains à impact social et environnemental. Ils aiment à s'appeler des « Blockchain Positivists ».

La **Fondation ELYX** sous l'égide de la Fondation Bullukian est reconnue d'utilité publique. Ses programmes ont pour vocation de faire de l'Agenda 2030 un succès, de participer à une culture ambitieuse et inclusive, et de valoriser l'innovation comme levier pour 2030.

L'Association Blockchain for Good *publie des analyses indépendantes et les opinions exprimées dans ce rapport n'engagent que leurs auteurs et ni les individus ou les organisations consultées, ni nos partenaires, l'Insitut Louis Bachelier, la chaire Blockchain@X de l'École Polytechnique, créé avec le soutien de Capgemini, NomadicLabs et la Caisse des dépôts et des Consignations, le Groupe Caisse des dépôts, la Banque Publique d'Investissement, PositiveBlockchain.io et la Fondation Elyx.*

CE CAHIER EST UN EXTRAIT DU RAPPORT :



LIBREMENT TELECHARGEABLE SUR BLOCKCHAINFORGOOD.FR

AUTEURS

Jacques-André Fines Schlumberger. Docteur en sciences de l'information et de la communication, après un Master de sciences politiques et une maîtrise de droit des affaires, Jacques-André Fines Schlumberger est entrepreneur, depuis les années 2000, sur des sujets d'innovations sociales et numériques. Il est enseignant à l'Université Panthéon-Assas (Paris 2) et auteur pour *La revue européenne des médias et du numérique*. Il s'intéresse aux blockchains et leurs applications pratiques depuis longtemps, et sous le prisme du développement durable depuis 2018.

Pierre Noro. Après plusieurs années passées au sein des programmes Blockchain et Cryptoactifs de la Caisse des Dépôts et des Consignations, Pierre Noro accompagne désormais des entreprises dans la conception et le développement de nouveaux services blockchain à impact social positif. Il est enseignant à Sciences Po Paris, au *Learning Planet Institute* (Université Paris-Cité) et chercheur. Outre ses travaux sur la gouvernance décentralisée et les problématiques éthiques dans le numérique, il collabore notamment au projet de vote en ligne décentralisé Pebble.vote.

Lucas Zaehringer. Co-fondateur de Positiveblockchain.io, Lucas Zaehringer explore les liens entre blockchain et impact social depuis 2017. Il est également *Lead Europe* chez Verity Tracking, une *startup* qui utilise la blockchain et la tokenisation pour décarboner les biocarburants et les chaînes de valeur biosourcées en lien avec les matières premières agricoles.

CONTRIBUTEURS

Pierre Champsavoir, Expert en gestion des risques et finance durable.
Noémie Dié, Doctorante en économie à Télécom Paris et Bpifrance Le Lab.
Alejandro Gómez, **Christophe Gbossou**, Membres experts, Africa 21.
Audran Gouis, Etudiant à Sciences Po Paris, Ecole d'Affaires Publiques.
Ani Ramos, Co-foundatrice de Positiveblockchain.io, Product Manager @Palm NFT Studio.
Razali Samsudin, Chercheur indépendant, Éducateur, Co-fondateur de Sustainable ADA.

RELECTEURS - CAHIER COMMUNICATION ÉLECTRONIQUE & TÉLCOS

Noémie Dié, Christophe Gbossou, Alejandro Gómez, Audran Gouis.

TABLE DES MATIÈRES

ACCÈS À INTERNET ---------- 9

INTERNET DES OBJETS (ET 5G) ---------- 15

RÉSEAU PRIVÉ VIRTUEL DÉCENTRALISÉ ---------- 18

ENJEUX ET QUESTIONS ---------- 23

GLOSSAIRE ---------- 25

ÉDITEUR ---------- 34

COMMUNICATION ÉLECTRONIQUE & TÉLÉCOMMUNICATION

Nombre de projets dans la base : 35

Nombre de projets actifs : 29

Nom des projets actifs : 3air ; Akash ; Althea ; BitClout ; Bitminutes ; Bitrefill ; Blockstack (formerly called OneName) ; Cajutel ; DAppNode ; Deeper Network ; Dent Wireless ; DFinity ; Filecoin ; Helium ; Holo ; HOPR ; KelVPN ; Kyve ; Maidsafe ; Mysterium Network ; NYM ; Orchid Labs ; RightMesh ; Skynet ; Stacks / Hiro;Substratum ; Syntropy ; Threefold ; World Mobile Token ; *vous ne trouvez pas votre projet ? Vous connaissez un projet qui ne figure pas dans l'annuaire ? Envoyez-nous un mail à* bonjour@blockchainforgood.fr.

Ce chapitre fait l'objet d'une publication en ligne ; si vous souhaitez échanger, annoter, corriger certaines informations, rendez-vous sur ce document : https://blockchainforgood.fr/index.php/1-2/

Et si « l'on changeait radicalement la logique qui sous-tend l'organisation des réseaux mondiaux ? Et si les utilisateurs eux-mêmes étaient au cœur des réseaux qu'ils utilisent ? Et si les blockchains servaient aussi à bâtir des infrastructures réseau et des protocoles plus libres, plus efficients et mieux sécurisés ? » s'interroge le journaliste Cyril Fievet[1].

En effet, l'infrastructure mondiale des télécommunications est aujourd'hui centralisée et repose sur une gestion de certaines fréquences radio à l'échelle de chaque Etat et d'un petit nombre d'opérateurs de télécommunications nationaux qui construisent les réseaux. Aujourd'hui, ces réseaux « *sous-tendent la plupart des applications dont nos sociétés sont devenues largement dépendantes en quelques décennies*[2] ». Les réseaux dits cellulaires de la 1G ou la 5G fonctionnent à l'international parce qu'ils sont normalisés et régulés sous l'égide de l'Union internationale des télécommunications, l'agence des Nations unies pour le développement spécialisée dans les technologies de l'information et de la communication.

Basée à Genève en Suisse, l'agence compte aujourd'hui 193 États membres et 900 entreprises, parmi lesquelles tous les opérateurs de télécommunication du monde, ainsi que des universités et des organisations internationales et régionales. Pour autant, plusieurs projets blockchain imaginent décentraliser l'accès à Internet, inventer des réseaux

1 « Demain, des réseaux vraiment décentralisés ? », Cyril Fievet, Clubic, 3 septembre 2021, https://www.clubic.com/technologies-d-avenir/dossier-381429-demain-des-reseaux-vraiment-decentralises-.html
2 « Les fréquences, gestion d'une ressource-clé », François Rancy, Annales des Mines Série « Enjeux numériques » N°9, Mars 2020, https://imtech.wp.imt.fr/2020/03/13/les-frequences-gestion-dune-ressource-cle/

distribués de télécommunication, et s'assurer que les principes de la neutralité du réseau Internet et de l'anonymat soient respectés en utilisant leurs services.

Mais comment décentraliser une infrastructure mondiale de réseau ? Car la raison pour laquelle les télécommunications *via* réseaux cellulaires sont régulées depuis 1865 est double. Le spectre des fréquences radioélectriques constitue une ressource rare, c'est-à-dire que les fréquences qui permettent d'établir une communication électronique sans fil, sur un réseau cellulaire, bien qu'instantanément renouvelables, ne sont disponibles qu'en quantité limitée à un moment donné. Et d'autre part, ces réseaux, d'un point de vue matériel, sont très coûteux à construire.

De 1976 à 2020 se sont succédées cinq générations de réseaux cellulaires : La première génération, dite 1G, date des années 1980 et inaugure l'usage de la voix en situation de mobilité, dans les années 1990. La deuxième génération, la 2G, voit se développer l'usage des SMS, la troisième génération, 3G, dans les années 2000, inaugure l'usage du Web en situation de mobilité, et dix ans plus tard, la 4G a fait basculer la voix sur IP et augmenter les débits. La 5G, quant à elle, entérine l'usage d'un réseau mondial de communications électroniques reposant sur la virtualisation logicielle de fonctions matérielles. L'histoire des réseaux cellulaires de 1976 à 2020 aura donc consisté en l'abandon progressif des technologies téléphoniques au profit des technologies informatiques pour établir une communication dorénavant électronique, les réseaux de cinquième génération en étant la consécration.

Ainsi, depuis 2013/2014, des projets blockchains ont essaimé dans les domaines de (1) l'accès à Internet, la télévision numérique et la téléphonie sur IP, (2) des réseaux bas-débit dédiés à l'Internet des objets, (3) des réseaux privés virtuels (Virtual Private Network - VPN). Fondée en 2013 à San Francisco aux Etats-Unis, Helium est un réseau sans fil pair-à-pair opérant dans le domaine de l'Internet des objets. De plus, et même si le projet est encore à l'état d'ébauche, la communauté autour de la blockchain publique **Helium** s'interroge à propos des opportunités d'adapter leur réseau décentralisé à (4) la 5G.

Que change vraiment la 5G ?

La 5G n'est pas une simple amélioration des réseaux de quatrième génération. Sa mise en œuvre repose « sur ***une architecture informatique où des équipements de réseaux sont remplacés par des serveurs spécialisés et des logiciels*** ». Plus précisément, l'Association nationale de la recherche et de la technologie (ANRT[3]) explique que « dans un réseau 5G, de nombreuses fonctions réseau

3 Créée en 1953, l'Association nationale de la recherche et de la technologie (ANRT) rassemble les acteurs publics et privés de la Recherche et développement (R&D) en France.

seront virtualisées, c'est à dire qu'elles s'exécuteront en tant que logiciel (monde informatique) », fournissant alors les services d'un « réseau sans fil privatif ».

Sur ce « réseau sans fil privatif » à très haut débit, les entreprises deviennent alors « conceptuellement leur propre opérateur mobile sur une zone géographique clairement circonscrite », sans toutefois devenir un opérateur de télécommunications au sens de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP[4]).

Parce que les données sont alors traitées séparément de celles du « réseau public, la protection, la confidentialité des données liées aux processus et à la production devient théoriquement totale ». Ou tout du moins la valeur des données échappe totalement à l'opérateur de télécommunications et revient à l'industriel qui gère lui-même ce réseau, mais également à ses éventuels prestataires, spécialistes des données et des communications électroniques.

Accès à Internet

L'Objectif de développement durable 9, « *mettre en place une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation*[5] », précise à la cible 9.c, qui vise expressément l'accès aux technologies de l'information et de la communication, vouloir « *accroître nettement l'accès aux technologies de l'information et de la communication et faire en sorte que tous les habitants des pays les moins avancés aient accès à Internet à un coût abordable d'ici à 2020*[6] ».

En 2019, l'UNICEF et l'Union internationale des télécommunications ont lancé **Giga**, avec pour objectif de « *fournir de la connectivité* [au réseau Internet] à toutes les écoles du monde ».

En 2020, 40 % de la population mondiale, 3,2 milliards de personnes, ne peut pas se connecter à Internet, parmi lesquelles 1 milliard se trouvent en Asie du Sud, et 870 millions en Afrique.

Le projet de Giga est de (1) cartographier[7] la connectivité des écoles dans les pays en développement, (2) connecter toutes les écoles et les communautés aux

4 Créée par la loi du 26 juillet 1996, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) est une autorité administrative indépendante française chargée de réguler les communications électroniques et postales et la distribution de la presse.
5 Objectif de développement durable 9 : Bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation https://www.un.org/sustainabledevelopment/fr/infrastructure/
6 *Ibid*.
7 « Mapping School Connectivity Globally », UNICEF, retrieved May 16, 2022, https://projectconnect.unicef.org/map

alentours, (3) financer la connexion au réseau et (4) créer un écosystème propice à l'éducation et au travail[8].

Pour mener à bien cette cartographie, Giga teste la connectivité des écoles à travers un système de suivi en temps réel dont les informations sont enregistrées dans une blockchain publique afin de « *réduire la possibilité que les informations aient été falsifiées par l'école, le fournisseur d'accès à Internet ou un autre tiers* ».

En 2021, un million d'écoles sur les six millions que visent le projet ont été cartographiées. Elles sont réparties dans 41 pays parmi lesquels le Kenya, le Rwanda, la Sierra Leone, le Kyrgyzstan, le Kazakhstan, l'Uzbekistan, le Salvador, le Honduras ou encore le Brésil. 44 % des écoles cartographiées ne disposent pas de connexion à Internet. Dans un second temps, lorsqu'une école est connectée à Internet, Giga s'assure que la connectivité est maintenue, notamment à travers des *smart contracts** qui permettent de « *gérer la relation, la conformité de l'accord et l'exécution avec le fournisseur de services Internet*[9] » et prévenir par exemple, lorsqu'une école n'est plus connectée pendant plus de 10 jours.

Sous certaines conditions le *smart contract** pourra enclencher le paiement du Fournisseur d'accès à Internet (FAI) local lorsque celui-ci fait défaut.

Giga pourra également offrir aux individus « *la possibilité d'établir une réputation au-delà des frontières de manière décentralisée* », notamment à travers la fourniture de certificats numériques[10] attestant d'une formation, permettant ainsi de « *débloquer l'accès à de nouveaux services tels que les services bancaires ou l'identification informelle* ». (voir Chapitre « Emploi & Formation »).

Giga travaille notamment sur ce sujet avec l'entreprise blockchain OS City, créée en 2016 à Mexico, qui déploie des infrastructures distribuées de services publics pour les gouvernements. Pour financer une partie de l'investissement nécessaire à la mise en place de Giga, l'Unicef a lancé depuis janvier 2022, en collaboration avec Snowcrash Labs[11], une collection de jetons non-fongibles (NFT*) intitulée « Patchwork Kingdoms[12] »,

8 « Bringing Connectivity to Schools in a Fair & Transparent Way Exploring where blockchain and Giga intersect », Christina Lomazzo, & Mehran Hydary, UNICEF.org, December 4, 2020, https://www.unicef.org/innovation/stories/blockchain-school-connectivity
9 *Ibid*.
10 « Exploring Blockchain for certification », UNICEF, retrieved May 17, 2022, https://certificates.unicef.io/
11 « Introducing birds of Solis », Snowcrash, retrieved July 8, 2022, https://snowcrash.com/
12 « Patchwork Kingdoms », GIGA, retrieved July 8, 2022, https://www.patchwork-kingdoms.com/

représentant chacun une école (voir image *supra*). Cette vente de NFT sert à médiatiser le projet tout en récoltant des fonds dont le produit servira à financer le programme de connectivité.

La *startup* **3air** s'intéresse au problème d'accès à Internet en Afrique, notamment parce que les infrastructures de réseau nécessitent des investissements bien plus élevés qu'ils n'existent de financement. Leur idée est de remplacer la mise en place d'un réseau d'accès filaire qui arrive au domicile de chacun par un réseau Internet envoyé *via* une station émettrice et réceptionné à l'aide de paraboles.

La station émettrice, appelée «K3 last mile», est une technologie brevetée appartenant à l'opérateur de télécommunications suisse K3 Telecom. Une station serait en mesure de fournir une connexion Internet allant jusqu'à 1Gb/s jusqu'à 50 km de distance et accueillir jusqu'à 15 000 internautes par station.

Le recours à une blockchain permettrait de gérer les identités numériques des utilisateurs, effectuer des transactions sans passer par un établissement bancaire et un certain nombre de services parmi lesquels « *la fidélisation et le parrainage des clients, la gouvernance et la création de communautés, les microcrédits, l'Internet des objets et d'autres fonctionnalités importantes orientées vers les télécommunications* ». 3air devait être construit sur la blockchain publique **Cardano** et utiliser le système d'identité décentralisée **d'Atala Prism**. Mais face à la pénurie de compétences techniques, l'entreprise a choisi de migrer vers une autre blockchain, **SKALE network**, qui tente d'améliorer la sécurité et la décentralisation des applications basées sur Ethereum.

L'infrastructure physique de réseau a déjà été déployée aux Etats-Unis, au Canada, en Espagne, en République Tchèque, en Slovénie, en Mauritanie, au Libéria et en Sierra Leone, l'un des pays les plus pauvres d'Afrique. Une offre initiale de jetons (ICO), visant à accélérer le développement de l'entreprise, notamment dans d'autres pays africains, a été reportée plusieurs fois. La plateforme développée par 3air s'adresse aux Fournisseurs d'accès à Internet (FAI) et opérateurs de télécommunication locaux en leur offrant un système « clef en main » pour la souscription de nouveaux clients, le suivi de l'état des abonnements et des solutions de paiement *via* blockchain.

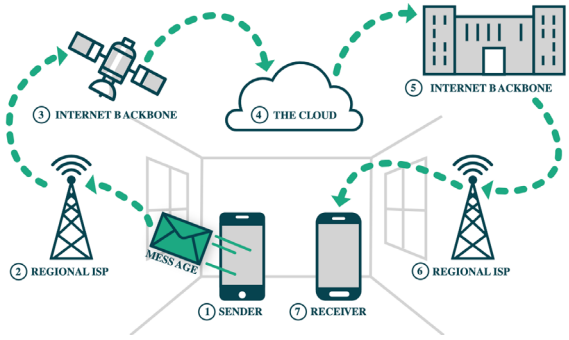
Le système de 3air simplifie la gestion du service et automatise les procédures administratives chronophages. Il s'appuie également sur un système de gestion d'identité décentralisée qui empêcherait l'exploitation des données personnelles des utilisateurs à leur insu (voir Chapitre « Identité et propriété »).

Cette initiative vise tout particulièrement les pays qui ne disposent pas d'un système bancaire opérationnel ni d'infrastructures de réseau développées. 3air imagine également pouvoir établir et

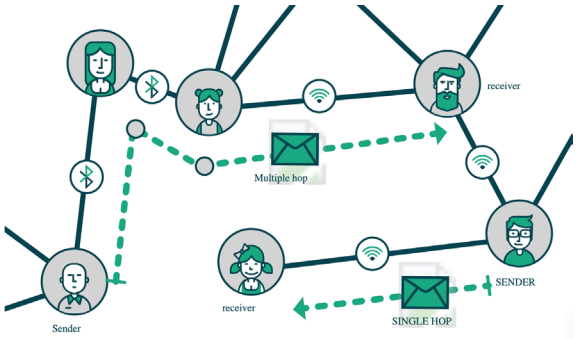
suivre des scores de crédit de l'utilisateur qui pourrait ensuite servir à mettre en place des systèmes de prêt au sein ou même en dehors de la plateforme[13]. L'infrastructure blockchain est utilisée pour permettre à un FAI ou un autre opérateur de gérer de nouveaux clients, qui devront générer une identifiant décentralisé auprès de l'opérateur, ce qui semble cependant exclure les personnes ne disposant pas de preuve de leur identité (voir Chapitre Identité et propriété).

Fondée au Canada en 2014 mais dont l'activité a cessé en 2019, **RightMesh** se présentait comme une entreprise blockchain qui « *rend la connectivité du dernier kilomètre abordable en utilisant des smartphones pour créer des réseaux maillés mobiles* ». Dans le domaine des télécommunications, le « dernier kilomètre » désigne l'écart entre l'infrastructure d'un fournisseur d'accès à Internet (FAI) et le domicile ou lieu de travail d'un client. Incubée de 2014 à 2018 par l'entreprise canadienne Left, RightMesh AG est aujourd'hui basée à Zoug en Suisse, et semble arrêtée. RightMesh a travaillé sur un projet au Bangladesh pour former des réseaux maillés mobiles en établissant et en gérant des connexions d'appareil à appareil entre des téléphones Android ou des appareils IoT*. Les connexions sont formées grâce aux technologies inhérentes à l'appareil, telles que Bluetooth, le Wi-Fi et le Wi-Fi Direct.

La proposition de RightMesh était la suivante :



Réseau traditionnel[14]



Réseau RightMesh[15]

Une fois qu'un appareil était connecté au réseau maillé, il pouvait envoyer et recevoir des données de l'une des deux manières suivantes : soit en un seul « saut » directement d'un dispositif à un autre, soit en mode « multi-sauts », les données étant transférées par de nombreux dispositifs jusqu'à ce qu'elles atteignent leur point d'arrivée. Cette méthode aurait également permis la livraison de messages hors ligne sur de plus grandes distances. Des tests et projets pilotes ont été menés au Bangladesh entre 2018 et 2020 avant que le projet ne s'arrête[16].

13 « White paper », 3air, retrieved June 8, 2022, https://docs.3air.io/pdf/3air_whitepaper.pdf
14« Rightmesh », Rightmesh, Medium, retrieved May 17, 2022, medium.com/rightmesh/
15 *Ibid.*
16 *Ibid.*

Althea, une entreprise américaine basée dans l'Oregon, se présente dans son livre blanc daté de 2017[17] comme un protocole de réseau maillé incitatif (*incentivized mesh network protocol*). C'est un fournisseur d'accès à Internet alternatif qui se concentre sur le problème du « dernier kilomètre » (voir *supra*). Les zones qui n'offrent pas de connexion Internet s'appellent des zones blanches. Althea Network utilise la technologie blockchain pour « *découpler les couches de service et d'infrastructure de la fourniture d'Internet, en donnant aux utilisateurs finaux la possibilité de partager les revenus en hébergeant l'infrastructure du réseau* ».

Ils mettent ainsi en œuvre un réseau maillé qui s'appuie sur des routeurs achetés par des particuliers, qui deviennent des opérateurs de réseau. Un réseau maillé correspond à une topologie de réseau où tous les hôtes sont connectés en pair-à-pair, sans point central de contrôle, et assurent ainsi le transfert de données entrantes et sortantes. Les réseaux locaux d'Althea sont ainsi constitués de nœuds appartenant aux personnes qui les utilisent et les réseaux sont gérés localement et gouvernés par la communauté de leurs utilisateurs.

Ces routeurs « *se payent mutuellement de la bande passante en utilisant des canaux de paiement en crypto-actifs*[18] ». Au-dessus de ce réseau de routeurs et de transfert de données, Althea construit un système permettant aux consommateurs de payer pour l'accès à Internet. Le système est construit sur la blockchain **xDai**, une blockchain de deuxième niveau (layer 2) sur la blockchain Ethereum, permettant d'opérer des microtransactions quasiment sans frais. Déjà déployé localement aux Etats-Unis, Althea, en partenariat avec Hub Advanced Networks, ont annoncé en décembre 2021 construire ce type de réseau maillé sur l'île de Porto Rico afin d'assurer la connectivité à Internet dans des zones reculées.

ThreeFold[19], créé en 2017, est une infrastructure de réseau Internet pair-à-pair et autonome (*Peer-To-Peer and autonomous Internet Grid*) qui n'utilise pas les traditionnels protocoles TCP/IP, utilisés pour le transfert des données sur Internet. L'infrastructure de réseau repose, en juin 2022[20], sur 3 100 nœuds, appelés 3Nodes. Ces serveurs fonctionnent avec un système d'exploitation *open-source* appelé Zero-OS et sont gérés par des personnes ou des organisations indépendantes appelées ThreeFold Farmers («*Farmers*») ; il existe même un guide[21] pour que quiconque puisse créer

17 Althea, « White paper », Github, retrieved July 8, 2022, https://github.com/althea-net/althea-whitepaper/blob/master/whitepaper.pdf
18 « Althea Network », Althea, retrieved July 8, 2022, https://www.althea.net/
19 « Learn How to build the people's Internet », Threefold, retrieved May 17, 2022, https://library.threefold.me/info/threefold#/
20 « ThreeFold Explorer », Threefold, retrieved July 8, 2022, https://explorer.threefold.io/all
21 « DIY Nodes Guide », Threefold, retrieved July 8, 2022, https://forum.threefold.io/t/diy-nodes-guide/837

simplement un serveur 3Nodes. Chaque 3Nodes fournit trois fonctions primitives de capacité de stockage, de capacité de calcul (sous la forme de conteneurs) et de capacité réseau (pour l'exécution des services réseau) et sont rémunérées en token (TFT) selon leur participation au réseau en termes de capacité (calcul, stockage, réseau).

Les ThreeFold Farmers génèrent des tokens appelés TFT qu'ils reçoivent en proportion de leur participation à l'infrastructure. Enfin, les utilisateurs dépensent des tokens TFT pour utiliser des capacités de calcul, de stockage et de réseau de manière modulaire, sur un registre distribué de type blockchain. Créé en 2017 sur la blockchain **Rivine** de **ThreeFold**, TFT est un token utilitaire qui permet ainsi à ses détenteurs d'utiliser la capacité Internet du ThreeFold Grid pour stocker leurs données et pour créer des applications.

Depuis la version 3.0 de ThreeFold, mis à jour en août 2021, toutes les activités stockage, de capacité de calcul et de capacité réseau, la facturation, le suivi de l'utilisation, l'identité et l'approvisionnement sont gérés sur la blockchain publique Stellar à travers le token TFT. En juin 2022, ThreeFold propose ainsi 84 Petabytes de capacité de stockage en ligne répartis dans 80 pays à travers le monde et sécurisés *via* 1 230 ThreeFold Farmers.

Syntropy, créé en février 2018, se présente également comme « *un projet ouvert fournissant une technologie de connectivité de nouvelle génération pour Internet* », alimenté par le token NOIA. Le livre blanc décrit le projet comme « *un écosystème et une plateforme composés de logiciels libres qui optimisent et cryptent le trafic Internet à l'aide de bibliothèques de cryptage modernes, de relais cryptés, soutenus par un grand livre distribué basé sur la blockchain. Collectivement, ces technologies servent de base à un réseau sécurisé et une économie du partage au-dessus des services Internet public existant*[22] ».

22 « A business case for an Internet Blockchain », William B. Norton, June 2, 2021, Syntropy Net, https://www.syntropynet.com/docs/Internetblockchain

Internet des objets (et 5G)

L'Internet des objets désigne ce paradigme où le réseau Internet et les capacités computationnelles de l'ordinateur (émettre, recevoir, traiter des données) se répand dans les objets, les lieux et les environnements physiques. Cette connectivité au réseau trouve des applications dans des domaines variés, parmi lesquels l'habitat, l'agriculture, la santé, le transport ou encore l'énergie. Alors que les réseaux cellulaires des opérateurs de télécommunication offrent des débits de plus en plus rapides mais de plus en plus coûteux, d'autres types de réseau dit bas-débit se sont développés, et sont exclusivement consacrés à la communication des objets *via* Internet.

Ces réseaux étendus à basse consommation (*Low Power Wide Area Network ou* LPWAN) sont employés comme réseau pour l'Internet des objets (Internet of Things - IoT) et dans la communication machine-à-machine. Ils reposent sur des bandes de fréquences ultracourtes (Ultra Narrow Band - UNB) qui ne sont pas régulées par l'Union internationale des télécommunications et transporte de petites quantités de données (quelques Ko) sur de longues distances (quelques dizaines de kilomètre) tout en sollicitant peu d'énergie[23].

Créé en 2013 par Shawn Fanning, un ancien de Napster, Amir Haleem, et Sean Carey, **Helium** est un réseau bas débit sans fil décentralisé (*decentralized wireless network*) à destination du marché de l'Internet des objets. Leur livre blanc, publié en novembre 2018, explique vouloir créer un réseau pour permettre « *aux appareils partout dans le monde de se connecter sans fil à Internet et de se géolocaliser sans avoir besoin d'outils de localisation par satellite très consommateurs en énergie ou de forfaits cellulaires coûteux* ».

Helium a développé le protocole Helium Wireless, WHIP, un « *protocole de réseau sans fil, bidirectionnel, sécurisé, de longue portée et de faible puissance, compatible avec une large gamme d'émetteurs-récepteurs radio existants fonctionnant dans le spectre de fréquences sans licence* ».

C'est un système de transfert de données bidirectionnel entre les dispositifs sans fil et l'Internet *via* un réseau de fournisseurs indépendants où : (1) les appareils paient pour envoyer et recevoir des données sur Internet et se géolocaliser, (2) les mineurs gagnent des token pour assurer la couverture du réseau, et (3) les mineurs gagnent des honoraires sur les transactions, et pour valider l'intégrité du réseau Helium.

Le réseau distribué s'appuie sur la « preuve de couverture de réseau » - *Proof of Coverage*, où les tokens HNT sont émis en tant que récompense auprès des participants faisant fonctionner les points d'accès du réseau. De décembre 2021 à juin 2022, le réseau est passé

23 En 2009, un dispositif Sigfox consommait 1 000 fois moins d'énergie qu'un dispositif GSM.

de 417 000 à 846 551[24] points d'accès (Hotspot) répartis dans 176 pays et dont les données peuvent être suivies en temps réel sur http://explorer.helium.com/hotspots.

Le 14 avril 2021, la communauté Helium a voté[25] pour travailler sur une évolution du réseau qui permettrait, à long terme, de **construire un réseau 5G décentralisé sur le même principe**. En août 2021, Helium a levé 111 millions de dollars lors d'une vente de token dirigée par Andreessen Horowitz, un fonds américain de capital-risque.

A notre connaissance, c'est le premier projet blockchain qui vient challenger le caractère industriel et centralisé des nouveaux opérateurs de données, rendus possibles par la 5G, un marché colossal qui suscite également la convoitise des trois premiers fournisseurs de services de *cloud* mondiaux, Amazon, Microsoft et Google, appelés *hyperscalers*[26].

24 « DISH First Major Carrier to Bring Helium 5G to the People », Amir Haleem, Helium, October 26, 2021, helium.com

25 HIP 27, un « *mécanisme économique permettant de prendre en charge de nouveaux protocoles sans fil sur le réseau Helium, à commencer par le LTE et la 5G dans la bande de spectre Citizens broadband radio service (CBRS)#.* Selon les développeurs d'Helium, « *la tarification des données ainsi que l'algorithme et le modèle économique de vérification de la couverture en radio fréquence (proof-of-coverage) qui fonctionnent bien pour LoRaWAN ne sont pas idéalement adaptés à d'autres protocoles sans fil tels que 5G, LTE, Wi-Fi, etc* ».

26 « *Parce qu'ils deviendraient tout à la fois des ressources clés de la 5G et qu'ils sont "détenteurs" des données de leurs "services gratuits" diffusés sur le web, Google.com, Facebook, Amazon, ces hyperscalers ne devraient être « considérés comme des compétiteurs comme les autres* », estime l'Association nationale de la recherche et de la technologie (ANRT). Source : « La 5G dans les chaines de valeur des données – Un défi technologique et industriel devant nous », ANRT, Pierre Bitard, mars 2021, https://www.anrt.asso.fr/sites/default/files/5g_chaine_de_valeur_des_donnees_anrt_futuris_2021_mars.pdf

L'écosystème technique d'Helium (Extrait du livre blanc « Helium A Decentralized Wireless Network »).

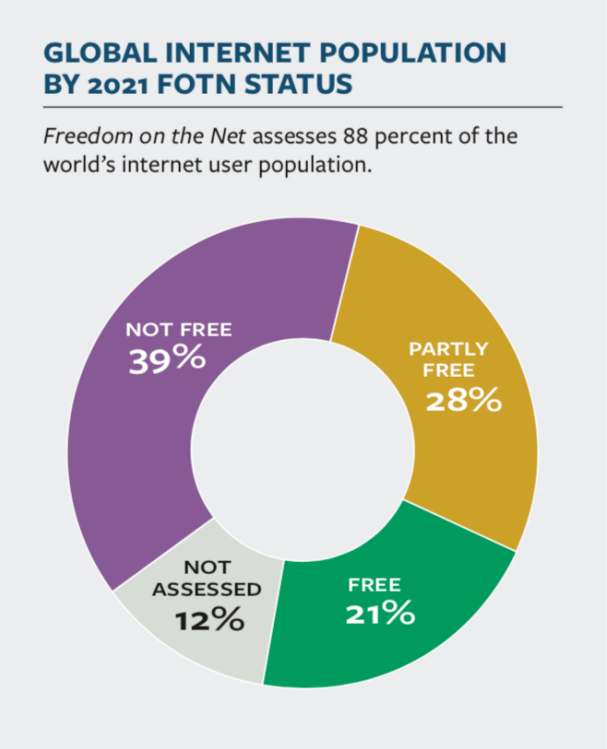
Le réseau Helium est un réseau sans fil décentralisé construit autour de WHIP sur une blockchain spécialement conçue à cet effet, avec un token natif, le NHT.
- Les appareils se présentent sous la forme de matériel contenant une puce radio et un micrologiciel compatible avec WHIP, et dépensent des tokens en payant des mineurs pour envoyer des données vers et depuis Internet.
- Les mineurs gagnent des tokens en fournissant une couverture de réseau sans fil par le biais d'un matériel spécialement conçu pour faire un pont entre WHIP et les routeurs, qui sont des applications Internet.
- Les dispositifs stockent leurs clés privées dans du matériel de stockage et leurs clés publiques dans la blockchain. Les mineurs rejoignent le réseau en affirmant leur localisation par satellite, un type spécial de transaction dans la blockchain, et en déposant un token.
- Les mineurs précisent le prix qu'ils sont prêts à accepter pour le transport des données et les services de preuve de localisation, et les routeurs précisent le prix qu'ils sont prêts à payer pour les données de leur dispositif. Les mineurs sont payés une fois qu'ils ont prouvé qu'ils ont livré les données au routeur spécifié du dispositif.
- Les mineurs participent à la création de nouveaux blocs dans la blockchain en étant élus *via* le mécanisme de consensus *asynchronous Byzantine Fault Tolerance* (aBFT*). Ils font alors partie du groupe de consensus.
- Les mineurs élus sont récompensés par de nouveaux tokens de protocole lors de la création de nouveaux blocs.
- La probabilité pour un mineur d'être élu parmi le groupe de consensus à une époque donnée est basée sur la qualité de la couverture du réseau sans fil qu'il fournit.
- La blockchain utilise la « preuve de couverture » (« *proof-of-coverage* », ou PoC) pour garantir que les mineurs représentent honnêtement la couverture du réseau sans fil qu'ils créent.

Extrait de « *Helium A Decentralized Wireless Network* » Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, Rahul Garg. Helium Systems, Inc. Release 0.4.2 2018-11-14 whitepaper.helium.com —

Réseau privé virtuel décentralisé

Le réseau Internet est un bien commun, disponible et ouvert à tous. La neutralité du réseau est le principe informatique qui vise à exclure *toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau pour s'assurer que les utilisateurs ne feront face à aucune gestion du trafic Internet qui aurait pour effet de limiter ou d'améliorer leur accès aux applications et services distribués sur le réseau*. En 2009, Benjamin Bayart, militant pour les libertés fondamentales dans la société de l'information et ingénieur français, a proposé quatre principes essentiels à la neutralité du Net[27] : (1) transmission des données par les opérateurs sans en examiner le contenu (2) transmission des données sans prise en compte de la source ou de la destination des données (3) transmission des données sans privilégier un protocole de communication (4) transmission des données sans en altérer le contenu.

Selon l'Organisation non gouvernementale Freedom House,« *la liberté sur Internet dans le monde a reculé pour la 11e année consécutive, les plus fortes détériorations ayant été enregistrées au Myanmar (Birmanie), au Belarus (Biélorussie) et en Ouganda* ». L'ONG a récemment publié leur rapport annuel à propos de la liberté sur Internet (voir image[28]) et révélé que sur les « *70 pays que couvrent le rapport, 48 pays, qui représentent 88 % des internautes dans le monde – ont imposé de nouvelles règles aux entreprises technologiques en matière de contenu, de données ou de concurrence au cours de l'année écoulée*[29] ».



De nombreux internautes, notamment dans les pays sujets à la censure et au filtrage du réseau Internet, utilisent un réseau privé virtuel pour pouvoir se connecter à des sources d'information ou utiliser des services interdits par leur gouvernement. Un réseau privé virtuel

27 « Table ronde politique : Neutralité du Net, liberté d'expression sur Internet...le Paquet Télécom et la loi HADOPI », Benjamin Bayart, April, 9 juillet 2009, https://www.april.org/transcription-table-ronde-politique-des-rmll-2009

28 « Freedom on the Net 2021 », Grant Baker, Cathryn Grothe, Amy Slipowitz, Manisha Vepa, Kian Vesteinsson, and Tessa Weal, Freedom House, 2021, https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

29 *Ibid.*

(en anglais *Virtual Private Network* - VPN) est un logiciel installé sur l'ordinateur ou le smartphone de son utilisateur qui redirige le trafic Internet *via* un tunnel sécurisé, masquant l'adresse IP et chiffrant ses données. Utiliser un VPN présente notamment l'intérêt d'échapper à la censure mise en place par un Fournisseur d'accès à Internet (FAI) ou par un État autoritaire[30].

Avec des centaines d'offres de logiciels VPN gratuits ou payants sur le marché, il est difficile de choisir un service en connaissance de cause, d'autant plus que de nombreux scandales ont émaillé la réputation de ces logiciels. Selon une étude conduite en 2020 par TheBestVPN[31], parmi les 115 VPN étudiés, 26 collectaient des données permettant d'identifier les utilisateurs, notamment les adresses IP, les lieux, les données relatives à la bande passante et les horodatages de connexion. Plus intriguant encore, le modèle économique de certains VPN gratuits, vantés pour assurer une connexion sécurisée et anonyme, reposent en réalité sur le vente des données personnelles de leurs utilisateurs.
Parce qu'un VPN repose sur un opérateur central qui gère les serveurs sur lesquels les données transitent, des projets blockchains se sont développés pour le remplacer par une architecture distribuée afin de garantir techniquement que la connexion au réseau est sécurisée et protégée. Werner Vermaak, journaliste pour CryptoSlate, définit un VPN décentralisé comme une « *connexion Internet sécurisée gérée par un réseau de nœuds, qui reçoivent une compensation pour maintenir leurs services et assurer la sécurité du réseau. Les VPN décentralisés fonctionnent différemment des services VPN ordinaires, car ils n'ont normalement pas de fournisseur central qui gère le réacheminement du trafic Internet*[32] ».
Les VPN décentralisés fonctionnent à travers des applications décentralisées - *decentralized applications* (dApps)*, qui permettent au réseau d'être sécurisé et à l'utilisateur, à partir de son navigateur web, de sélectionner les nœuds à travers lesquels sa connexion sera cryptée.

Nym, Mysterium Network, **Deeper Network**, **HOPR**[33], **KelVPN** ou encore **Orchid Labs** sont quelques-uns de ces VPN décentralisés. Mysterium Network, créé en 2017, revendique être passé de quelque 6 500 nœuds actifs en novembre 2021 à plus de 20 000 nœuds

30 Selon l'Association, FreedomHouse.org, les pays suivants filtrent intégralement les connexions Internet qui entrent et sortent de leurs frontières : China, Iran, Myanmar, Cuba, Vietnam, Saudi Arabia, Pakistan, Egypt, Ethiopia, United Arab Emirates, Uzbekistan, Venezuela, Russia, Bahrain, Belarus, Kazakhstan, Sudan, Turkey, Azerbaijan, Thailand, Rwanda.
31 « 100+ VPN Logging Policies Debunked », Rob Mardisalu, TheBestVPN, January 6, 2020, https://thebestvpn.com/118-vpns-logging-policy/
32 « VPNs for data privacy », Erner Vermaak, CryptoSlate, April 18, 2021, https://cryptoslate.com/the-5-best-decentralized-vpns-for-data-privacy/
33 HOPR, créé à Zurich en Suisse en 2020 se présente comme « *un protocole général de la couche réseau pour permettre aux utilisateurs d'échanger des données en privé, dans la même veine que Tor (le routeur oignon) ou un réseau privé virtuel (VPN)* »#. Le réseau est encore en phase de test.

actifs en juin 2022 répartis dans plus de 120 pays, pour un trafic mensuel de données dépassant les 700 Terabytes et presque 67 000 sessions quotidiennes[34]. **Deeper Network**, fondé en 2019 à Santa Clara aux Etats-Unis, revendique quant à lui 65 000 nœuds répartis dans plus de 200 pays[35].

Orchid Labs, créé[36] en 2017 à San Francisco aux Etats-Unis, se présente comme « *un système décentralisé et ouvert de communication anonyme et de réseau privé virtuel (VPN - Virtual Private Networking), comprenant un marché de bande passante où les fournisseurs de nœuds mettent en jeu une monnaie numérique pour annoncer leurs services en utilisant la blockchain Ethereum et reçoivent un paiement en OXT (la crypto-actif native d'Orchid)* ». Orchids Labs a créé un écosystème de VPN décentralisé reposant sur (1) une application pour ordinateur et smartphone, disponible gratuitement pour l'utilisateur, (2) un token appelé OXT, (3) un système de comptes Orchid pour assurer leur confidentialité, (4) un système de nanopaiement, (5) un système de noeuds (nodes) et (6) un système de *staking**.

Le token OXT, un token ERC-20* sur la blockchain Ethereum, sert de monnaie numérique entre des fournisseurs et des utilisateurs de bande passante. Les fournisseurs de bande passante, tous indépendants les uns des autres, sont les nœuds du réseau (*nodes*). Le système est ouvert pour que n'importe qui puisse exploiter un nœud Orchid, à charge de détenir des tokens OXT.

En effet, la blockchain Orchid s'appuie sur la preuve de détention pour sécuriser les transactions opérées sur le réseau. Plus un utilisateur détient d'OXT et de nœuds, plus les chances d'être récompensé pour valider des blocs de transactions sur le réseau sont grandes.

De son côté, l'utilisateur paye, à l'échelle du « nano paiement », en tokens OXT ou dans une autre crypto-actif prise en charge, le temps passé à utiliser la connexion Internet sécurisée.

Comme le paiement se fait au temps passé, Orchid utilise une architecture de paiement appelée «*nano-paiements probabilistes pour les paiements de réseau par paquet*[37]». Ces nanopaiements sont opérés sur la blockchain Orchid pour éviter les problèmes de congestion et de frais du réseau Ethereum. Le montant minimum pour commencer à utiliser le VPN décentralisé d'Orchid Labs est de un dollar. Une autre fonctionnalité permet aux utilisateurs d'acheter des

34 « Mysterium makes the Internet blind to borders », Mysterium, retrieved May 17, 2022, mysterium.network
35 « Deeper Network Basic Mining 2.0 + Mining updates for Genesis and Basic Mining, Deeper Network May 13 https://deeper-network.medium.com/deeper-network-basic-mining-2-0-mining-updates-for-genesis-and-basic-mining-2ec2f112cfd4
36 Par Dr. Steven Waterhouse, Jay Freeman, Brian J. Fox, Gustav Simonsson, et Stephen Bell.
37 « Introducing Nanopayments », Orchid, October 9, 2019, https://medium.com/orchid-labs/probabilistic-nanopayments-4aa423c3f22f

« crédits Orchid » en monnaie fiduciaire*, ces tokens OXT ne pouvant alors plus être retirés et convertis ailleurs, mais seulement dépensés auprès des fournisseurs du réseau. La place de marché sur laquelle se rejoint l'offre et la demande est décentralisée et fonctionne en pair-à-pair, ce qui garantit à l'utilisateur l'efficience du service.

Autre exemple, la *startup* **NYM**, basée à Neuchâtel en Suisse développe également depuis 2018, une infrastructure de réseau « *confidentielle, open source, décentralisée et sans permission* » en fournissant un système de confidentialité dit *full-stack*, que l'on peut traduire par « clef en main ».

Pour ses fondateurs, la confidentialité sur Internet est « *minée par une collecte de données omniprésente et des monopoles centralisés, ce qui empêche l'apparition de services et de plateformes innovants*[38] ». Pour y remédier, l'infrastructure de NYM permet « à d'autres applications, services ou blockchains de fournir à leurs utilisateurs une forte protection des métadonnées, à la fois au niveau du réseau (mixnet), et *au niveau de l'application (informations d'identification anonymes) sans avoir besoin de construire la confidentialité à partir de zé*ro ».

Nym est un réseau de niveau supérieur qui prend en charge les fonctions d'accès à des services en ligne afin d'être utilisées par des fournisseurs d'applications et leurs utilisateurs. Pour protéger les données qui circulent sur le réseau Internet public, le réseau Nym est composé d'un mixnet décentralisé (un réseau de nœuds de mixage), inspiré des travaux dans les années 1980 du cypherpunk David Chaum.

Sur un *mixnet*, les données de connexion sont regroupées en paquets, chiffrées successivement puis transférées de nœud en nœud (*mix nodes*) où chaque nœud ôte une couche de chiffrement, jusqu'à au dernier qui livre le message à son destinataire. De cette manière les connexions qui se font sur le réseau sont totalement anonymes, y compris pour les plus grands attaquants, capables de surveiller le réseau dans sa globalité.

Le réseau Nym compte 472 nœuds pour 13 passerelles et 27 validateurs en juin 2022[39]. Un fonctionnement technique proche du réseau Tor, un projet *open source* immatriculé en 2006 mais imaginé depuis les années 1990, notamment sous l'impulsion du laboratoire de recherche naval américain (NRL) qui cherchait alors un moyen « *d'acheminer le trafic à travers plusieurs serveurs et de le chiffrer à chaque étape*[40] » et protéger ainsi ses communications sur le réseau Internet naissant.

38 « White paper - « The Nym Network The Next Generation of Privacy Infrastructure », Claudia Diaz, Harry Halpin, and Aggelos Kiayias, Nym Technologies SA Version 1.0, Feb 26 2021, nymtech.net
39 « Overview », Nym Network explorer, retrieved Jun 8, 2022, https://explorer.nymtech.net/overview
40 The Tor Project, « History », https://www.torproject.org/about/history/

Pour utiliser le réseau Tor, une personne télécharge gratuitement le navigateur éponyme[41] dont le trafic passera par un minimum de trois nœuds relais avant d'atteindre un nœud de sortie final.

Alors que Tor est basé sur un réseau dont les nœuds pour acheminer le trafic sont bénévoles, le propre des réseaux VPN décentralisés est d'ajouter une incitation économique à la tenue d'un nœud par les opérateurs, rémunérés en crypto actifs.

Ce qui explique probablement qu'un VPN décentralisé comme Deeper Network, créé seulement en 2019, revendique 65 000 noeuds alors que le réseau Tor, au bout de 16 ans de services, n'en déploie que 6 400[42].

41 Download Tor Browser https://www.torproject.org/download/
42 Tor Metrics: https://metrics.torproject.org/

ENJEUX ET QUESTIONS

Les technologies de l'information et de la communication sont dorénavant des infrastructures essentielles au même titre que les routes, les réseaux d'assainissement ou encore l'énergie électrique.

De vastes infrastructures de réseau font encore défaut dans bon nombre de pays en développement, ce qui fait qu'en 2021, « *16 % de la population mondiale n'a pas accès aux réseaux haut débit mobiles*[1] » selon l'ONU.

L'ensemble des contraintes en matière d'infrastructures affectent la productivité des entreprises, « *d'environ 40 % pour de nombreux pays africains*[2] ».

Comme l'illustre le projet Giga de l'Unicef, le premier enjeu des communications électroniques est celui de l'accès à Internet, notamment dans les écoles, afin de permettre aux nouvelles générations de se former et de s'approprier les nouveaux usages du numérique.

L'infrastructure de réseaux permettant l'accès à Internet nécessite de très lourds investissements. Verra-t-on des initiatives blockchains permettant d'innover dans le domaine de l'accès à Internet, notamment par le développement de réseaux maillés ?

Le partage de données mobiles sur blockchain pose la question de l'accès à Internet, notamment dans les pays en développement. Il peut être une solution comme mentionné précédemment, mais cette solution repose principalement sur l'accès initial à un réseau mobile classique. Comment dès lors assurer une connexion de bonne qualité, en continu et à tous ?

Les services d'accès Internet sur blockchain peuvent-ils dès lors faire l'économie d'investissements infrastructurels plus importants dans ces pays ? Au contraire, peuvent-ils permettre de diminuer le nombre d'infrastructures nécessaires à assurer une bonne connexion réseau pour tous, permettant ainsi de diminuer le coût de ces investissements ?

Le développement des réseaux

1 Objectif de développement durable 9 : Bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation https://www.un.org/sustainabledevelopment/fr/infrastructure/
2 *Ibid*.

privés virtuels (VPN), utilisés pour pouvoir se connecter à des sources d'information ou utiliser des services de manière sécurisée rappelle combien les outils permettant d'échapper à la censure mise en place par des Fournisseurs d'accès à Internet (FAI) contrôlés par des Etats et à la surveillance des réseaux par des entreprises peu scrupuleuses sont nécessaires. Mais quelle en est l'accessibilité ? Ces services ne sont-ils pas réservés à une élite, formée et disposant d'un certain bagage technique ?

En effet, ces VPN décentralisés sont encore complexes à mettre en œuvre et à utiliser, note Louis Bertucci, chercheur à l'Institut Louis Bachelier[3]. « *Pour les rendre plus accessibles, il faudra une couche d'abstraction supplémentaire qui masquera l'utilisation de ces protocoles complexes. Nous pourrions faire le parallèle avec le réseau Internet lui-même. Internet est une succession de protocoles de communication complexes développés dans les années 1980. Cependant, l'adoption par le grand public est arrivée bien plus tard pour deux raisons : il a d'abord fallu construire l'infrastructure (les serveurs, les routeurs, etc.), puis attendre que des entreprises comme Microsoft, Google ou Amazon (pour AWS) voient le jour et permettent aux utilisateurs d'envoyer un mail par un simple clic à partir de leur machine* » poursuit-il.

Se passera-t-il la même chose avec ces technologies encore émergentes ?

3 Entretien avec Louis Bertucci. 30 juin 2022.

GLOSSAIRE

Altcoin : Un Altcoin désigne toutes les crypto-actifs alternatifs au bitcoin. Depuis la création du premier bitcoin en 2009, le site coinmarketcap.com en dénombrait 2 360 au 22 juillet 2019, 10 429 au 15 juin 2021 et 20 246 en juillet 2022.

AMM - *Automated Market Maker*. Voir "Teneur de Marché Automatisé".

API : En informatique, une interface de programmation applicative (en anglais *Application Programming Interface*) est un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle une blockchain va offrir des services à d'autres logiciels. Une API blockchain spécifie comment des programmes informatiques pourront se servir des fonctionnalités et des données distribuées accessibles dans le registre d'une blockchain.

Attestations vérifiables - *Verifiable Credential - (VC)* : preuves numériques délivrées par un tiers (appelé *issuer*) à un utilisateur (*holder*) prouvant une caractéristique de son identité (son âge, son lieu de naissance, …). Ainsi, en présentant ces attestations vérifiables à un vérificateur (*verifier*), l'utilisateur peut transmettre les informations strictement nécessaires pour accéder à un service tout en restant maître de ses données personnelles.

Atomic Swap : En finance, le *swap*, de l'anglais *to swap* – échanger, désigne un contrat d'échange financier. Dans le domaine des crypto-actifs, un Atomic Swap désigne une méthode d'échange de token en pair-à-pair. Cette méthode repose sur un *smart contract** spécifique appelé « contrats à empreinte numérique verrouillés dans le temps » (*hashed TimeLocked Contracts* (HTLCs). Le principe repose sur la garantie que les deux personnes qui échangent des tokens le feront réellement. Le *smart contract* requiert que le destinataire d'un paiement accuse réception du paiement dans un temps imparti, en générant un récépissé cryptographique. Si ce n'est pas le cas, le destinataire perd le droit d'accéder aux fonds qui sont alors retournés à l'expéditeur.

Arbre de Merkle ou **arbre de hachage** : En informatique et en cryptographie, un arbre de Merkel est une structure de données contenant un résumé d›information d'un grand volume de données. Le principe d'un arbre de hachage est de pouvoir vérifier l›intégrité d'un ensemble de données sans les avoir nécessairement toutes au moment de la vérification. Pour ce faire, au sein d'une série de données, l'une d'entre elles est hashée. Ce hash sera accolé à un hash d'une deuxième donnée issue de la même série. Cette concaténation va permettre de créer un hash parent. Le processus se répète avec les hash parents jusqu'à arriver à un hash unique, appelé le hash sommet. Ainsi, pour vérifier l'intégrité d'une donnée, il suffit de connaître le hash des données qui lui sont reliées.

Block Explorer : Voir “explorateur blockchain”.

CEX / DEX : *Centralized Exchange Platform / Decentralized Exchange Platform* - voir DEX.

Crypto-actif stable - *Stable coin* : crypto-actif collatéralisée par une monnaie fiduciaire ou sur un autre crypto-actif, respectant une parité fixe vis-à-vis de celle-ci ou celui-ci. Par exemple, le crypto-actif stable Dai de MakerDAO respecte une parité fixe vis-à-vis du dollar américain : 1 Dai = 1 USD. Il existe trois types de crypto-actifs stables, correspondant à trois moyens de respecter cette parité. D’une part, les crypto-actifs stables centralisés sont créés à partir de réserves en monnaie fiduciaire (par exemple, le dollar américain) déposées par les utilisateurs dans l’application et conservées en banque par les opérateurs du service. De fait, la quantité de crypto-actifs mise en circulation correspond exactement aux réserves de monnaie fiduciaire. D’autre part, les crypto-actifs stables décentralisés sont créés à partir de réserves dans d’autres crypto-actifs. Ainsi, les crypto-actifs stables sont créés en fonction de la valeur, en dollar, des autres crypto-actifs détenus en réserve. Le Dai de MakerDAO, précédemment mentionné, est un crypto-actif stable décentralisé. Enfin, il existe des crypto-actifs stables décentralisés algorithmiques, qui sont créés en fonction des variations d’une autre crypto-actif créé par le même opérateur de service. Cet autre crypto-actif sera émis et racheté de sorte à faire fluctuer le cours par rapport au dollar américain. Sa valeur en dollar permettra de créer des crypto-actifs stables. Ce processus a été très décrié notamment lors de l’effondrement du stablecoin algorithmique Luna/Terra.

dApps - *Decentralized Application,* Application décentralisée : Pour Andreas Antonopoulos[1], une application décentralisée inclut « *un ou plusieurs* smart contract *déployé(s) sur une ou plusieurs blockchain, une interface utilisateur transparente, un modèle distribué de stockage de données, un protocole de communication de messages de pair à pair et un système décentralisé de résolution de noms*[2] ». Une fois déployée sur une blockchain publique comme Ethereum, le code informatique d›une application décentralisée (dApp) ne peut être ni supprimé ni arrêté afin que quiconque puisse en utiliser les fonctionnalités. Cela veut dire que même si la personne ou le groupe de personne à l’origine de l’application disparaît, l’application décentralisée, quant à elle, continuera de fonctionner.

DAO - *Decentralized Autonomous Organization,* Organisation Autonome Décentralisée : Une DAO est une organisation de personnes fonctionnant

1 Auteur du livre de référence « Mastering Bitcoin 2nd Edition: Programming the Open Blockchain », 2017, O’Reilly, ISBN 978-1491954386
2 « Mastering Bitcoin - Second Edition », Andreas M. Antonopoulos, Creative Commons, retrieved Jun 15 2022, https://github.com/bitcoinbook/bitcoinbook

grâce à un programme informatique qui fournit des règles de gouvernance à la communauté sans direction centralisée. Ces règles sont transparentes et immuables parce que codées dans un protocole blockchain.

DeFi - *Decentralized Finance* : voir "Finance décentralisée"

Delegated Proof of Stake : voir "Preuve d'enjeu déléguée".

DEX - *Decentralized Exchange,* Échanges décentralisés : Un échange décentralisé (DEX) est un type d'échange de crypto-actifs qui fonctionne en pair-à-pair et sans intermédiaire. Contrairement aux plateformes d'échanges centralisées (CEX, *Centralized Exchange*), comme Binance ou Kraken, les échanges s'opèrent directement entre les utilisateurs, réduisant ainsi le risque de vol causé par le piratage des échanges, la manipulation des prix et garantissant un meilleur anonymat.

Explorateur de blockchain : Toute blockchain publique dispose d›une interface de ligne de commande (*Command line interface* - CLI) pour afficher l›historique des transactions sur le réseau. Afin de permettre à quiconque d'accéder à l'historique de ces transactions, la plupart des blockchains publiques proposent également un « explorateur » accessible *via* un navigateur web afin d'afficher de manière conviviale les informations recherchées. Voir par exemple https://www.blockchain.com/explorer.

Ethereum Virtual Machine - Machine Virtuelle Ethereum : entité virtuelle unique permettant l'exécution de tous les *smart contracts** de toutes les applications décentralisées (dApps) et de toutes les Organisations autonomes décentralisées (DAO en anglais) développées sur la blockchain publique sans permission Ethereum. En effet, Ethereum peut être comparé à un automate fini distribué. Un automate fini distribué est une construction mathématique pouvant changer d'état. Ethereum possède deux états : un état lui permettant de gérer tous les comptes et les soldes des paiements effectués avec son crypto-actif natif, l'Ether ; et un état appelé "état machine". Cet "état machine" change de bloc en bloc, de sorte à exécuter les *smart contracts** qui s'y trouvent. Les changements de l'état machine s'effectuent selon un ensemble de règles. Ces règles spécifiques de changement d›état de bloc à bloc sont définies par l›Ethereum Virtual Machine (ethereum.org).

Feature phone - *Téléphone basique* : Téléphone mobile possédant les caractéristiques techniques basiques d'un *smartphone*.

Fork (*hard* / *soft*) - Scission : En langage informatique, un *fork* consiste à créer un nouveau logiciel à partir du code source d'un logiciel existant. Un *soft fork* apporte des modifications à la blockchain concernée qui vont s'appliquer uniquement dans le futur, alors que les modifications introduites par un *hard fork* valent également pour le passé.

Un *hard fork* consiste donc à réécrire le code source d'un protocole blockchain après son lancement.

Finance Décentralisée - *Decentralized Finance (DeFi)* **:** La *DeFi* est un écosystème d'applications reproduisant des services financiers sur une blockchain. Elles permettent à quiconque en a les moyens et indépendamment du pays où il se trouve ou de sa nationalité, d'emprunter, prêter et investir, assurer et échanger des crypto-actifs sans passer par un intermédiaire, les transactions étant sécurisées via l'usage d'une blockchain et de *smart contracts.*

Hachage (fonction de) : fonction mathématique qui transforme n'importe quel contenu sous la forme d'un nombre hexadécimal. À la moindre modification du contenu, le nombre haché devient totalement différent. L'intérêt d'une fonction de hachage est qu'elle ne s'applique que dans un sens : le hachage obtenu ne permet pas de remonter au contenu d'origine, en revanche il suffit de hacher à nouveau ce contenu pour vérifier que le hachage en résultant est identique, preuve qu'aucune modification n'est intervenue. Les blocs de transaction d'une blockchain sont ainsi hachés au fur et à mesure et permettent d'avoir la garantie qu'ils n'ont jamais été modifiés depuis la première transaction.

ICO - *Initial Coin Offering,* Offre initiale de token : Émission de tokens échangeables contre des crypto-actifs pour lever des fonds auprès d'une communauté. Contrairement à une IPO (*Initial Public Offering*) qui permet la cotation des actions d'une société sur un marché boursier, une ICO n'est pas encadrée par un régulateur financier.

IPFS - *InterPlanetary File System* (IPFS), Système de fichier inter-planétaire : Un système distribué de fichiers pair à pair dont l'objectif est de stocker des informations et des données de manière décentralisée, sécurisée et confidentielle, permettant ainsi de se prémunir contre toute forme de censure. Aujourd'hui, une recherche d'information sur le web consiste à demander à un moteur de recherche "où se trouve le contenu" afin d'identifier l'URL du serveur où il se trouve ; une recherche dans l'IPFS consiste à demander au système "le contenu que l'on recherche", identifié par un hash cryptographique unique et permanent. Créé en 2014 par Juan Benet, IPFS est un protocole *open source* qui pourrait se développer à côté du protocole HTTP inventé par Tim Berners-Lee en 1991.

Lightning Network - réseau Lightning : Protocole de paiement de pair-à-pair construit comme une application de deuxième couche sur la blockchain Bitcoin qui permet d'opérer des transactions en bitcoin extrêmement rapides, de l'ordre d'un million par seconde, quasiment sans frais et sans dépense énergétique, puisque la validation des transactions ne nécessite pas de minage par la preuve de travail. Depuis 2015, des acteurs de la communauté Bitcoin, dont notamment

Lightning Labs, Blockstream et ACINQ, travaillent sur ce protocole qui apporte l'une des réponses au problème de changement d›ordre de grandeur(scalabilité) de Bitcoin qui, pour rappel, ne peut traiter que 7 à 10 transactions par seconde. Le réseau Lightning fonctionne depuis mai 2018.

Mainnet / Testnet : Le terme *mainnet* est utilisé pour décrire le moment où un protocole blockchain est entièrement développé et déployé, et que les transactions en crypto-actifs sont diffusées, vérifiées et enregistrées sur la blockchain. Le terme *testnet* décrit l'environnement de développement et de tests avant le lancement du *mainnet*.

Mineur : validateur de transactions sur une blockchain. Le mineur est rémunéré dans le crypto-actif natif de la blockchain au sein de laquelle il valide les transactions.

Monnaie fiduciaire - *fiat money* : Monnaie sous la forme de pièces et de billets, dont la valeur nominale est supérieure à la valeur intrinsèque. La confiance (*fiducia* en latin) que lui accorde l›utilisateur comme valeur d›échange, moyen de paiement, et donc comme monnaie repose sur le cours légal attribué par l'État.

NFT (Non-Fungible Token) : littéralement jetons non-fongibles. *A contrario* de deux pièces de monnaies fongibles, c'est-à-dire qui ne peuvent être différenciées (une pièce d'un euro ressemble en tous points à une autre pièce d'un euro), un NFT est un token unique, cette unicité lui faisant perdre son caractère fongible.

Un NFT exécute du code informatique stocké dans des *smart contracts** conformes à des normes différentes telles que ERC-721 sur Ethereum.

On Chain/Off Chain : Quand une transaction s'effectue *on-chain*, cela veut dire qu'elle est inscrite dans un bloc de transaction enregistré dans une blockchain. En revanche, une transaction *off-chain* se déroule en dehors de ladite blockchain. Par exemple, les transactions sur le Lightning Network (voir *supra*) sont effectuées en dehors de la blockchain de Bitcoin et sont dites *off-chain*.

Oracle : dans le domaine des blockchains, un Oracle est une source d'information provenant du monde physique sur laquelle est connecté un ou plusieurs *smart contracts* et dont les parties s'entendent sur la fiabilité des données. On peut prendre comme exemple l'IATA pour les données liées aux vols aériens ou encore Météo France pour les données liées à la météorologie (précipitation, gel, neige etc.). Utilisées dans le cadre d'applications décentralisées, les données d'un oracle permettent d'enclencher les termes d'un *smart contract*. Par exemple, une assurance paramétrique remboursera automatiquement un agriculteur en cas de perturbation météorologique dont les données sont certifiées par un oracle.

Phrase mnémotechnique - *Seed Phrase* **:** Suite de mots (généralement 12 ou 24) permettant la récupération d'un portefeuille de cryptomonnaies depuis n'importe quel appareil.

Pool de minage : association de mineurs coopérant pour la réalisation du travail de validation des transactions au sein d'une blockchain. Les gains effectués par les machines acquises en commun sont partagés entre les membres du *pool* de minage.

Portefeuille (de crypto-actifs), *Wallet* : en matière de crypto-actif, un portefeuille est un dispositif qui peut prendre la forme d'un support physique, d›un programme informatique ou encore d›un service, et dont l'objet est de stocker les clés publiques et/ou privées de crypto-actifs. Ce procédé de stockage de la clé privée, connue du seul propriétaire du portefeuille, permet à son détenteur de signer des transactions et de prouver à l'ensemble des pairs du réseau blockchain qu'il est bien le propriétaire des crypto-actifs utilisés.

Portefeuille d'identité - *Identity Wallet* : Portefeuille composé d'attestations vérifiables. Voir Attestation vérifiable

Preuve d'enjeu déléguée - *Delegated Proof of Stake* : Mécanisme de consensus réduisant le nombre de noeuds d'une blockchain et reposant sur l'élection de mineurs (les validateurs de blocs de transactions sur une blockchain) qui ont immobilisé des fonds (*stake*) en crypto-actifs dans une blockchain au prorata de ce que chacun possède.

Preuve à divulgation nulle de connaissance - *Zero Knowledge Proof* (ZKP) **:** Une preuve à divulgation nulle de connaissance est une méthode de chiffrement qui permet à une personne (le prouveur) de prouver à une autre personne (le vérificateur) qu›elle est en possession de certaines informations sans les révéler au vérificateur. En d'autres termes, la preuve à divulgation nulle de connaissance permet de présenter des preuves de faits portant sur des données personnelles sans pour autant révéler ces données personnelles. Les preuves à connaissance nulle ont été conçues pour la première fois en 1985 par Shafi Goldwasser, Silvio Micali et Charles Rackoff dans leur article «*The Knowledge Complexity of Interactive Proof-Systems*».

Proof-of-stake : Preuve d'enjeu, ou Preuve de participation. Méthode pour valider les blocs de transactions d'une blockchain imaginée par Scott Nadal et Sunny King en 2012. Cette méthode demande à l'utilisateur de prouver la possession d'une certaine quantité de crypto-actif pour prétendre pouvoir valider des blocs supplémentaires dans ladite blockchain et pouvoir percevoir la récompense à l'addition de ces blocs. Ce mécanisme de consensus consiste à résoudre un défi informatique appelé *minting* (monnayage), opéré par des « forgeurs ». Il ne nécessite pas de matériel informatique puissant, consomme peu d'électricité et tient sur un nano ordinateur comme le Rasperry Pi. Pour valider un bloc de transactions, le forgeur met en dépôt une certaine quantité de crypto-actifs et reçoit une récompense lorsqu'il valide un bloc pour le blocage de ce capital. Si le forgeur procède à une attaque informatique en insérant de faux blocs de transactions dans la blockchain,

la communauté, à partir du moment où elle s'en rend compte, pourrait procéder à un *hard fork**, ce qui entraînerait la perte des dépôts de l'attaquant. Vitalik Buterin, cofondateur d'Ethereum explique : « *la philosophie de la preuve d'enjeu résumée en une phrase n'est donc pas "*la sécurité vient de l'énergie dépensée*", mais plutôt "*la sécurité vient des pertes économiques engendrées par une attaque*"* ».

Proof of Authority (PoA) - Preuve d'autorité : La preuve d'autorité est un algorithme de consensus qui désigne un nombre restreint et identifié d'acteurs au sein d'un réseau blockchain ayant le pouvoir de valider les transactions et de mettre à jour le registre. Cet algorithme de consensus est souvent mis en œuvre sur des blockchains privées ou de consortium. L'intérêt pour ces acteurs, souvent bancaires, étant de gagner en auditabilité et ainsi de réduire et d'optimiser les coûts liés à leur coordination.

REDD + *Reducing Emission from Deforestation and Forest Degradation* : mécanisme mis au point par les parties prenantes à la Convention-cadre des Nations Unies sur les Changements Climatiques (CCNUCC), qui crée une valeur financière pour le carbone stocké dans les forêts en offrant aux pays en développement des incitations à réduire les émissions provenant des terres forestières et à investir dans des stratégies de développement durable à faibles émissions de carbone. Au-delà de la déforestation et de la dégradation des forêts, REDD + inclut le rôle de la conservation, de la gestion durable des forêts et de l›amélioration des stocks de carbone des forêts.

RFID : Identification par Radiofréquence, *Radio Frequency identification* : désigne une méthode d'identification de données à distance, incorporées, sous la forme de tag, dans des objets ou des produits et comprenant une antenne associée à une puce électronique.

Satoshi : Un Satoshi est la plus petite unité divisible d'un Bitcoin, soit le 8e chiffre après la virgule. Un satoshi est donc égal à 0,00000001 bitcoin. Le nom s'inspire du nom de la personne ou du groupe de personnes ayant publiés le livre blanc fondateur de Bitcoin en 2008.

SDK - *Software Development Kit*, Kit de développement logiciel : Ensemble d›outils d›aide à la programmation pour la conception et le développement de logiciels ou d›applications.

Seed Phrase - Phrase mnémotechnique : voir "phrase mnémotechnique".

Sidechain : Une *Sidechain* est une blockchain secondaire ou parallèle conçue pour fonctionner à côté d'une blockchain primaire, publique, afin d'en accroître les capacités et remédier à leurs limites inhérentes, notamment de mise à l'échelle (scalabilité). Le recours à une *Sidechain* permet de traiter des opérations sans solliciter la blockchain primaire afin, par exemple, de réaliser des calculs spécifiques, ou encore de traiter des *smarts contracts* dans un environnement privé avant que les données soient enregistrées dans une blockchain primaire, comme Bitcoin ou Ethereum.

Smart Contract : Selon le site Ethereum.org, les contrats intelligents sont « *des applications qui s'exécutent exactement telles que programmées, sans possibilité de les arrêter, non censurables, sans fraude possible et sans interférence de tierce partie* ». L'intérêt de ces contrats est qu'ils sont autonomes, automatiques et répliqués dans tous les nœuds d'une blockchain, et que leur exécution ne passe pas par un tiers de confiance pour en garantir la validité. Plusieurs blockchains publiques permettent de mettre en œuvre des *smart contracts*, dont notamment Ethereum, Polkadot, Tezos, Stellar ou encore Solana.

Staking : Le *staking* consiste, pour un utilisateur, à immobiliser et verrouiller des tokens dans un *smart contract*. Le protocole attribue de façon aléatoire à l'un des participants le droit de valider un bloc de transactions et recevoir une récompense en token. Le mécanisme de la "preuve de détention", *proof of stake* incite les utilisateurs à immobiliser leur token, la probabilité d'être choisi pour valider un bloc de transaction étant proportionnelle au nombre de tokens verrouillés. Plus l'utilisateur a de tokens verrouillés, plus la probabilité d'être choisi pour valider la transaction est grande. Si un utilisateur tente d'écrire de fausses transactions dans un bloc, il perd ses tokens immobilisés et se fait bannir du réseau.

Stablecoin : voir **"**Crypto-actif stable".

Teneur de marché automatisé : protocole permettant de calculer le taux de change entre deux crypto-actifs de manière automatique. Le teneur de marché automatisé est à la base de tous les DEX (*Decentralised Exchange*), et permettent à ses usagers d'échanger des crypto-actifs entre eux en pair-à-pair, sans passer par un tiers. La première plateforme à utiliser ce principe se nomme Uniswap.

Token / Tokenisation : Un token, jeton en français, est une unité (un actif) numérique échangé sur une blockchain. Le bitcoin est le jeton de la blockchain Bitcoin. L'Ether est le jeton de la blockchain Ethereum. Par extension, l'expression « tokenisation » désigne l'idée qu'un actif, quel qu'il soit, puisse être représenté numériquement et échangé *via* une blockchain.

Tolérance aux pannes byzantines *(Byzantine Fault Tolerance, BFT)* : La tolérance aux pannes byzantines est une solution au problème logique des généraux Byzantins. Ce problème logique, élaboré en 1982, consiste à expliquer les difficultés de coordination simultanée des actions de trois armées commandées par trois généraux alliés. En effet, ces derniers doivent attaquer ou battre en retraite en même temps. Or, un général ne peut connaître les actions des autres que par l'intermédiaire d'émissaires. Par conséquent, un général malveillant envoyant une information erronée aux deux autres brouillera les actions des alliés.

En appliquant cette situation aux réseaux informatiques, on peut en déduire que seulement un tiers des membres d'un réseau est capable de nuire à l'entièreté de ce dernier. La tolérance aux pannes byzantines est la capacité d'une technologie donnée de se prémunir contre ce type de comportement. Les mécanismes de consensus par la preuve de travail et par la preuve d'enjeu sont des exemples de solutions rendant les blockchains tolérantes aux pannes byzantines.

Tolérance aux pannes byzantines asynchrones (asynchronous Byzantine Fault Tolerance, aBFT) : La tolérance aux pannes byzantines asynchrones est une manière alternative de répondre au problème des généraux byzantins (voir *supra*). Plutôt que de faire en sorte que les trois généraux soient coordonnés en permanence, il s'agit de confier la direction des trois armées aux généraux bienveillants, tout en excluant le général malveillant du contrôle de son armée. Du point de vue d'un réseau informatique, un réseau tolérant aux pannes byzantines asynchrones authentifie les membres bienveillants de ce dernier pour leur confier la responsabilité de le faire fonctionner.

Wallet - Portefeuille : voir "portefeuille d'identité"

Zero Knowledge Proof - Preuve à divulgation nulle de connaissance. Voir "Preuve à Divulgation Nulle de Connaissance".

Rapport publié par l'Association Blockchain for Good
Directeur de la publication : Jacques-André Fines Schlumberger - Septembre 2022
bonjour@blockchainforgood.fr

Pour citer ce rapport : « *Rapport Blockchains & développement durable* », Association de loi 1901 Blockchain for Good - France, Jacques-André Fines Schlumberger Ph.D., septembre 2022.