

ENVIRONNEMENT & CLIMAT

SEPTEMBRE 2022

WWW.BLOCKCHAINFORGOOD.FR



BLOCKCHAIN
@POLYTECHNIQUE

bpifrance
SERVIR L'AVENIR



Caisse
des Dépôts
GROUPE

INSTITUT
Louis Bachelier

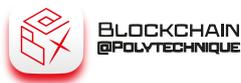
PB PositiveBlockchain.io

A PROPOS



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



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).



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'Institut 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 :

Blockchains & développement durable

2022

BLOCKCHAIN FOR GOOD **BLOCKCHAIN @POLYTECHNIQUE** **bpifrance** **Caisse des Dépôts GROUPE** **INSTITUT Louis Bachelier** **PositiveBlockchain.io**

LIBREMENT TELECHARGEABLE SUR [BLOCKCHAINFORGOOD.FR](https://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 Zaehringier. Co-fondateur de *Positiveblockchain.io*, Lucas Zaehringier 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-fondatrice de *Positiveblockchain.io*, Product Manager @Palm NFT Studio.

Razali Samsudin, Chercheur indépendant, Educateur, Co-fondateur de Sustainable ADA.

RELECTEURS - CAHIER ENVIRONNEMENT & CLIMAT

[Louis Bertucci](#), [Noémie Dié](#), [Patrice Geoffron](#), [Audran Gouis](#), [Stéphane Voisin](#).

TABLE DES MATIÈRES

CLIMAT ET RÉDUCTION DU CARBONE -----	9
POLLUTION ET DÉCHETS -----	20
VIE AQUATIQUE -----	23
EAU ET ASSAINISSEMENT -----	24
ENJEUX ET QUESTIONS -----	27
GLOSSAIRE -----	30
ÉDITEUR -----	40

ENVIRONNEMENT ET CLIMAT

Nombre de projets dans la base : 101

Nombre de projets actifs : 67

Nom des projets actifs : 1PLANET Marketplace ; Arup water exchange ; Atato ; Avano ; BFlo ; BICOWG ; Brokoli Network ; Carbonfuture GmbH ; CarbonX ; Carbonized.xyz ; Changeblock ; Chooose ; Circularise ; Civic Ledger ; Climate Futures ; ClimateDAO ; Climatetrade ; CO2DAO ; CO2ken ; Coorest ; Cut.eco ; DAO IPCI ; dclimate ; Diatom ; DOVU ; Earthbanc ; ecoriseDAO ; Eden DAO ; Empower ; EthaVerse ; Evergreen Coin ; Excess Materials Exchange ; Farm ; Flow Carbon ; Gainforest ; Green World Campaign;»International Platform for Insetting (IPI)» ; Inuk;klimaDAO ; Moonjelly DAO ; Nori ; Open Earth Foundation ; Open Forest Protocol ; OpenSurface ; Pacifical ; Plastic Bank ; PlastiCoin ; PlataformaVerde ; Porini.Foundation ; PoseidonFoundation ; Proyecto Colmena ; RECDefi ; Regen.network ; Reneum (Sindicatum Blockchain Technologies) ; Solarfullcycle ; Solid World DAO ; Sustainable Bitcoin Standard ; TerraBioDAO ; Toucan Protocol ; TREECYCLE ; Treejer ; UPCO2 ; Veridium Labs ; Verity Tracking ; Wood Tracking Protocol ; Wren ; Zero Carbon Project ; *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/>

Pour certains, associer blockchains et environnement est un oxymore. Pourtant, un double mouvement semble actuellement à l'œuvre : le premier vise à décarboner le secteur des blockchains et le second tient à l'accélération d'un certain nombre d'initiatives dont l'objectif est de lutter contre le changement climatique et préserver l'environnement.

Conscients des questions environnementales et écologiques qu'ils suscitent, certains acteurs des

blockchains œuvrent à décarboner le secteur. C'est l'objectif affiché du *Crypto Climate Accord*, initié en 2021 par Energy Web, le Rocky Mountain Institute (RMI) et le promoteur de systèmes financiers équitables Alliance for Innovative Regulation (AIR), rejoint depuis par plus de 250 acteurs du marché. L'ambition commune est de décarboner le secteur mondial des crypto-actifs en « *donnant la priorité à la gestion du climat et en soutenant la transition de l'ensemble du secteur de la crypto vers des émissions nettes de gaz à effet de*



serre nulles d'ici 2040¹ ». Deux objectifs intermédiaires sont prévus : d'une part, « atteindre des émissions nettes nulles de la consommation d'électricité pour les signataires du Crypto Climate Accord d'ici 2030² », et d'autre part, « élaborer des normes, des outils et des technologies avec les membres du Crypto Climate Accord afin d'accélérer l'adoption et la vérification des progrès vers des blockchains alimentées à 100 % par des énergies renouvelables d'ici la conférence COP30 de la Convention-cadre des Nations unies sur les changements climatiques en 2025³ ».

En amont de cette initiative récente, il importe de souligner que la question du climat et de l'environnement anime la communauté crypto, et au-delà, depuis plusieurs années. Le *Blockchain & Climate Institute* (BCI), basé à Londres depuis 2016, est un groupe de réflexion et d'action qui vise à faciliter la mise en œuvre de l'accord de Paris. De même, la *Climate Chain Coalition* est une organisation au statut d'observatoire officiel de la Convention-cadre des Nations unies sur les changements climatiques (UNFCCC), créée à Paris en décembre 2017, et dont le siège est à Ottawa au Canada et qui – forte 170 membres à travers 44 pays – vise à mobiliser le financement climatique et améliorer les mécanismes dits de Mesure, Rapport et Vérification ((*Measurement, Reporting and Verification* - MRV) afin d'intensifier la lutte contre le changement climatique.

Une autre tendance observable tient à la multiplication de projets blockchain dédiés à lutter contre le changement climatique et à la préservation de l'environnement.

Et, dans ce champ, la variété des projets mérite d'être soulignée : décentralisation de marchés volontaires de carbone, de marchés de l'eau, financement de collectes de déchets, dons en crypto-actifs fléchés vers des projets environnementaux ou bien encore projets d'agroécologie et de reforestation. Les sujets de décentralisation des échanges énergétiques, des certificats d'énergie (économies, garanties de *sourcing* renouvelable, ...) et l'optimisation du réseau, sont abordés dans le chapitre intitulé « Énergie ». Le chapitre « Monnaie électronique pair-à-pair et argent programmable » traite, en outre, de la finance dédiée au développement des énergies renouvelables.

1 Crypto Climate Accord : <https://cryptoclimate.org/accord>. consulté le 31 mai 2022.

2 *Ibid.*

3 *Ibid.*

Climat et réduction du carbone

Le marché carbone est l'une des pierres angulaires de la politique énergie-climat de l'Europe depuis 2005, date du lancement du Système communautaire d'échange de quotas d'émission – en anglais *European Union Emissions Trading System* (EU ETS⁴). Depuis, le nombre de marchés de quotas d'émission dans le monde est en constante augmentation, notamment aux Etats-Unis depuis 2009, mais aussi au Canada, en Australie, en Chine, au Japon, en Nouvelle-Zélande, en Corée du Sud, en Suisse, ainsi qu'en Chine pour ne citer que les principaux marchés.

Le 14 juillet 2021, la Commission européenne a adopté une série de propositions législatives exposant la manière dont elle entend atteindre la neutralité climatique dans l'Union européenne d'ici 2050. Aujourd'hui, le système communautaire d'échange de quotas d'émission s'applique à 11 000 installations européennes, responsables d'environ 50 % des émissions de CO₂ et 40 % des émissions de gaz à effet de serre générées globalement dans l'Union européenne⁵.

Ce marché carbone est destiné à l'échange de crédits carbone, avec l'objectif de

fournir des incitations économiques à la réduction des émissions. Chaque unité de crédit représente la réduction ou l'élimination d'une tonne d'équivalent CO₂ de l'atmosphère. Cela inclut également le carbone séquestré ou évité grâce à la mise en œuvre du projet. Il existe deux types de marchés : (1) Ceux qui présentent un caractère obligatoire (dits de « conformité ») – dont les participants, à l'échelle de pays et d'industries, sont assujettis à une limite d'émissions – (2) et ceux qui procèdent d'une démarche volontaire, ne sont pas réglementés par une autorité publique, mais sont toutefois régis par des administrateurs de standards de certification des réductions d'émissions de carbone, tels que le Verified Carbon Standard⁶ (Verra), l'American Carbon Registry⁷, ou encore le Gold Standard⁸.

Sur les marchés volontaires de carbone, il n'y a pas de limite au nombre de crédits carbone générés par des projets climatiques à impact positif que d'autres pourront acheter pour compenser leurs émissions.

C'est sur ces marchés que les blockchains se sont invitées : *« de nombreux projets Web3 innovent dans la chaîne de valeur du carbone, car les blockchains améliorent intrinsèquement la transparence,*

4 « EU Emissions Trading System (EU ETS) »; European Commission, retrieved May 16, 2022, https://ec.europa.eu/clima/eu-action/eu-emissions-trading-system-eu-ets_en

5 « Marchés du carbone > Le système européen d'échanges de quotas d'émissions de gaz à effet de serre (SEQE) », Ministère de la transition énergétique, 20 décembre 2021, <https://www.ecologie.gouv.fr/marches-du-carbone>

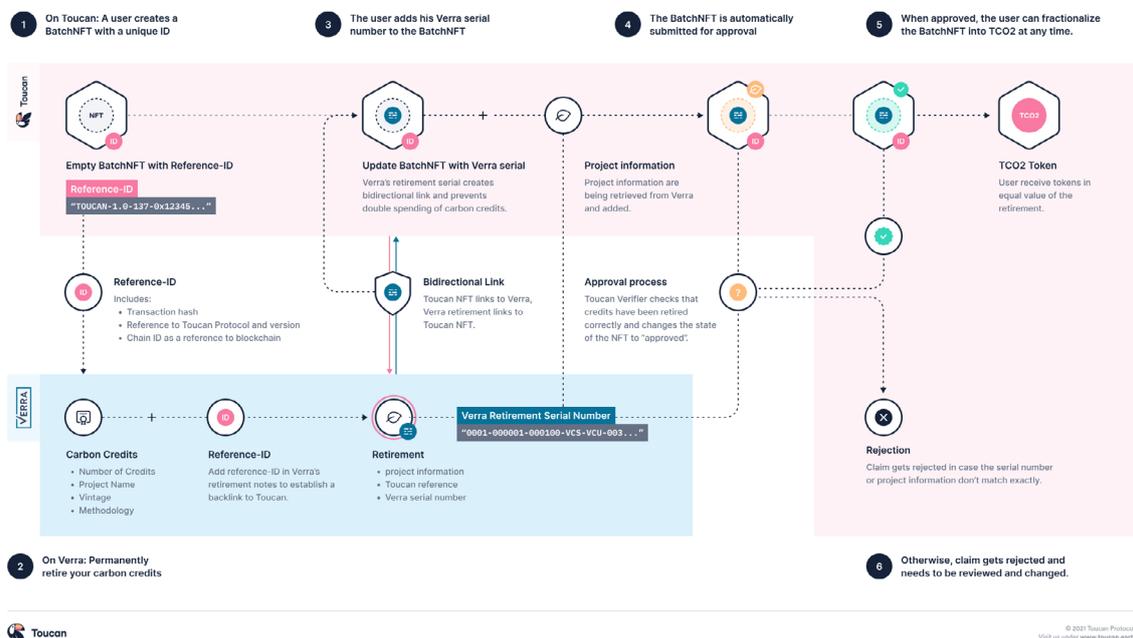
6 Verra: <https://verra.org/project/vcs-program/>

7 American Carbon Registry: <https://americancarbonregistry.org/>

8 Gold Standard: <https://www.goldstandard.org/>



How does the Carbon Bridge work?



« How does Carbon Bridge Work », Toucan Protocol.

Source : Toucan Protocol, May 16 2022, <https://docs.toucan.earth/protocol/bridge/carbon-bridge>

la traçabilité, la programmabilité et la négociabilité des compensations de carbone » explique Louise Borreani de Curve Labs⁹.

Toucan Protocol, Nori, le Cambridge Centre for Carbon Credits, Moss, Klima DAO, Climate Trade ou encore **Wren** ou **CO²DAO** sont quelques-uns de ces projets qui viennent fluidifier les marchés volontaires de carbone traditionnels, au nombre d'une vingtaine en 2020 selon le rapport publié par « *l'International Carbon Action Partnership Status Report*¹⁰ ».

Toucan Protocol, créé en 2020, se définit comme « *une infrastructure de marché pour amener les marchés du carbone sur les blockchains publiques* ». Le protocole permet à quiconque de tokeniser* ses crédits carbone, inscrits sur le registre Verra, et de les rendre disponibles dans le monde émergent de la finance décentralisée¹¹ (DeFi*), comme l'illustre le partenariat entre Toucan Protocol et **Celo** (voir *infra*). Le protocole, *open source*¹², met en oeuvre un « Carbon Bridge » et le token Base Carbon Tonne (BCT), autrement dit une

9 « Cybernetic solutions for the distributed economy », Curve Labs, retrieved May 16, 2022, <https://blog.curve Labs.eu>

10 « Emissions Trading Worldwide: Status Report 2020. Berlin: International Carbon Action Partnership », ICAP, 2020, https://icapcarbonaction.com/system/files/document/200323_icap_report_web.pdf

11 Voir Chapitre « Monnaie électronique pair-à-pair et argent programmable ».

12 « Smart contracts of the Toucan Protocol », Github, retrieved May 16 2022, <https://github.com/ToucanProtocol/contracts>

passerelle des crédits carbone (Verified Carbon Units / VCUs) issus du registre Verra¹³ vers la blockchain publique de Toucan Protocol (le token BCT). Construit sur la blockchain Polygon¹⁴, le protocole Toucan déploie un ensemble de *smart contracts*¹⁵ qui garantissent tout à la fois la provenance des crédits carbone, et permettent également d'en assurer une plus grande liquidité, en les réunissant dans des fonds communs (*carbon pools*). Ces nouveaux instruments financiers sont rendus disponibles dans toutes les applications de la Finance décentralisée construite autour de l'écosystème Ethereum. Le mécanisme de consensus de la blockchain publique repose sur la preuve de détention*, est également compatible avec d'autres applications comme **Klima DAO** dont nous parlerons plus loin.

En mai 2022, 18,3 millions de tonnes de crédits carbone provenant du registre Verra, correspondant à 167 projets climats ont ainsi été tokenisés sur la blockchain de Toucan Protocol¹⁶ et disponibles à l'écosystème de la Finance décentralisée. **Celo**¹⁷, une blockchain

publique sans permission - qui s'adresse tout particulièrement aux populations qui sont exclues du système bancaire traditionnel et permet à quiconque possédant un smartphone d'envoyer et recevoir des crypto-actifs et des crypto-actifs stables* (dollars, euros et Real) - a noué un partenariat avec Toucan Protocol en avril 2022. Toucan et Celo projettent de créer un pont Celo-Polygon en collaboration avec Curve Labs pour permettre aux utilisateurs de transférer leurs tokens Base Carbon Tonne (BCT) et Nature Carbon Tonne (NCT), entre Celo et Polygon. Une fois ce pont créé, Toucan sera lancé sur la blockchain Celo et permettra à quiconque appartenant à l'écosystème « *d'accéder, de déposer dans des pools et de retirer des TCO2 (crédits carbone tokenisés) et d'échanger des BCT et NCT contre des jetons carbone détenus dans des pools*¹⁸ ». Celo projette également de lancer à l'avenir un « *programme de subventions destiné à augmenter le nombre de projets ReFi*¹⁹ dans l'écosystème Celo²⁰ ».

Créé en 2017, **Nori** se présente, dans son livre blanc daté de 2019²¹, comme

13 « Verified Carbon Units (VCUs) », Verified Carbon Standard, retrieved May 16, 2022. <https://verra.org/project/vcs-program/verified-carbon-units-vcus/>

14 Polygon est une solution de mise à l'échelle de type « layer two » ou « sidechain » qui fonctionne parallèlement à la blockchain Ethereum, permettant des transactions rapides et des frais réduits.

15 Les mots marqués d'un astérisque renvoient vers le glossaire.

16 « Carbon On-Chained », Toucan Protocol, retrieved May 16, 2022, <https://toucan.earth/>

17 Voir Chapitre « Monnaie électronique pair-à-pair et argent programmable » et <https://celo.org/>

18 « The Celo Foundation, Climate Collective, and Toucan Collaboration Deepens to Bring ReFi to the Masses » Celo Foundation, Apr 11 2022. <https://medium.com/celoorg/the-celo-foundation-climate-collective-and-toucan-collaboration-deepens-to-bring-refi-to-the-e714700b96d0>

19 Finance régénérative ; voir notamment « The Promises and Pitfalls of Regenerative Finance Towards a Critical Yet Constructive Dialogue », Curve Labs Curve Labs, May 23, 2022, <https://blog.curvelabs.eu/the-promises-and-pitfalls-of-regenerative-finance-4910f0f6f690>

20 *Ibid.*

21 Nori, « white paper », https://storage.googleapis.com/nori-prod-cms-uploads/white_paper_e567a48109/



« une place de marché basée sur la blockchain pour éliminer le dioxyde de carbone de l'atmosphère » en s'appuyant sur l'agriculture dite « régénératrice ».

L'agriculture régénératrice

Source : Novethic, consulté le 16 Mai 2022, <https://www.novethic.fr/lexique/detail/agriculture-regeneratrice.html>

Cette approche est constituée d'un ensemble de méthodes d'agriculture – inspirées notamment par la paysannerie traditionnelle et la permaculture – ayant pour but de régénérer les sols dégradés, d'augmenter la biodiversité et de lutter contre les changements climatiques en favorisant la rétention du dioxyde de carbone. De cette façon, l'agriculture régénératrice contribue à réduire les niveaux de CO² engendrés par l'utilisation d'engrais minéraux et de produits agrochimiques. L'agriculture régénératrice repose essentiellement sur l'élimination du labour qui détruit les sols ; la mise en place de cultures de couverture et intercalaires, la rotation des cultures et l'application de compost permettant d'augmenter biologiquement la fertilité des sols ; le maintien de la biodiversité et la régénération des sols grâce à la restauration de la flore bactérienne ; le recours au pâturage. L'agriculture régénératrice associe productivité et protection des écosystèmes sur le long terme.

Nori a mis en place un certificat de suppression du carbone (Carbon Removal Certificates - CRC) à partir de *smart contracts** basés sur la blockchain Ethereum, représentant un token correspondant à une tonne de CO² supprimée. Ce certificat de suppression du carbone est créé à partir d'une version modifiée de la norme de jeton non fongible ERC-721, en combinaison avec la norme de jeton avancé ERC-777 qui lui confère des propriétés de non fongibilité, permettant à la fois de distinguer chaque certificat et de les rendre divisibles pour gagner en liquidité²².

La place de marché Nori met ainsi en relation (1) des agriculteurs qui s'engagent à des pratiques régénératrices en fournissant les données historiques de leurs projets. (2) Des vérificateurs tiers qui « *légitiment ensuite ces données en s'assurant qu'elles sont raisonnables, légalement autorisées et qu'elles ne figurent pas dans d'autres registres. Ensuite, un outil de quantification tiers crée des estimations de suppression de carbone qui informent la génération de token NRT de Nori. Enfin, (3) les acheteurs peuvent acheter des tonnes de suppression de carbone Nori (NRT) auprès des fournisseurs*²³ ». Nori a ainsi vendu plus de 78 000 tonnes de CO² éliminées et a rémunéré quelque 1,3 millions de dollars aux agriculteurs qui ont mis en œuvre de telles pratiques.

white_paper_e567a48109.pdf

22 « A blockchain-based marketplace for removing carbon dioxide from the atmosphere. Version 3.0.1 », NORI, February 18, 2019, https://storage.googleapis.com/nori-prod-cms-uploads/white_paper_e567a48109/white_paper_e567a48109.pdf

23 « Our Mission is to reverse Climate Change », NORI, retrieved May 16, 2022, <https://nori.com/litepaper>

Le caractère ouvert et décentralisé des blockchains publiques sans permission permet à quiconque de construire d'autres initiatives s'appuyant sur leur architecture décentralisée, comme, par exemple, KlimaDAO.

KlimaDAO, à ne pas confondre avec ClimateDAO, est une Organisation autonome décentralisée (DAO*) et un protocole de finance décentralisée (DeFi) mettant en œuvre un token appelé KLIMA. Ce dispositif fonde un marché carbone décentralisé et ouvert, conceptualisé et construit par une équipe distribuée et pseudo-anonyme²⁴, inspiré d'OlympusDAO (autre protocole DeFi ayant déjà attiré plus de 500 millions de dollars depuis sa mise en œuvre en mai 2021, hébergé sur la blockchain Ethereum, et qui vise à créer une réserve monétaire adossée à un panier de crypto-actifs). L'objectif de KlimaDAO est « *d'encourager la réduction des émissions en faisant monter le prix des actifs carbone*²⁵ ». Un procédé à rapprocher des « investisseurs activistes », des investisseurs qui achètent des actions dans le but de gagner en influence et de faire pression sur la direction d'une entreprise afin qu'elle oriente sa stratégie selon leurs revendications. La banque Lazard, qui

procède à un décompte annuel de ces fonds, estimait à 42 milliards de dollars en 2021 les « *participations minoritaires au capital de sociétés cotées supposées mal gérées en s'efforçant de peser sur leur stratégie*²⁶ ».

Selon l'équipe de KlimaDAO, « *plus l'externalité négative de leurs dommages devient coûteuse, plus la décision de réduire les émissions et d'investir dans des solutions vertes est rentable* ». Autrement dit, le mécanisme de KlimaDAO consiste à retirer des crédits du marché volontaire du carbone et à les placer dans la trésorerie de la DAO*, avec pour effet d'augmenter les coûts des compensations carbone et de les rendre plus élevés pour les entreprises à forte intensité de carbone.

KlimaDAO, *open source*²⁷, met en œuvre un token ERC20 selon la norme Ethereum, appelé KLIMA, indexé au token BCT (Base Carbon Tonne) correspondant à un crédit – équivalent à une tonne de carbone – émis sur la blockchain de Toucan Protocol (voir *supra*), provenant des Verified Carbon Units (VCUs) de Verra. Ces tokens KLIMA sont notamment échangeables sur la plateforme d'échange décentralisée* (DEX) **Sushiswap**. Ils sont bloqués

24 Le pseudo-anonymat permet à quelqu'un de publier et de commenter de manière anonyme, sans qu'un identifiant soit visible, les informations le concernant étant en la possession du fournisseur du service ou l'administrateur du site web.

25 What is Klima DAO and How Does it Work ?, retrieved May 16, 2022, <https://www.coingecko.com/buzz/what-is-klima-dao-and-how-does-it-work>

26 « Les Fonds activistes ont davantage choisi leurs cibles », Guillaume Bayre, TradingSat, 6 février 2022, <https://www.tradingsat.com/actualites/marches/en-2021-les-fonds-activistes-ont-davantage-choisi-leurs-cibles-1004759.html>

27 « KlimaDAO », Github, retrieved May 16, 2022, <https://github.com/KlimaDAO/klimadao>



dans la trésorerie de Klima DAO et leurs détenteurs votent sur la politique de l'Organisation autonome décentralisée*. KlimaDAO joue ainsi, selon leurs termes, de « *banque dé-centrale en régissant la politique monétaire de cette nouvelle monnaie adossée au carbone, tout comme une banque centrale régit la politique monétaire d'une monnaie fiduciaire*²⁸ ». La DAO* a acquis en peu de temps plus de 120 millions de dollars de compensations de carbone *via* Toucan Protocol.

Selon le cabinet McKinsey, le prix de la tonne de carbone a vocation à croître dans les années à venir, de sorte que « *la demande de crédit carbone pourrait être multipliée par un facteur de 15 ou plus d'ici 2030 et par un facteur allant jusqu'à 100 d'ici 2050*²⁹ », pour un marché estimé à 50 milliards de dollars en 2030. Klima DAO prend le pari qu'il sera prochainement plus rentable pour des entreprises générant trop d'émissions de modifier leurs pratiques que de compter sur le rachat de crédits carbone.

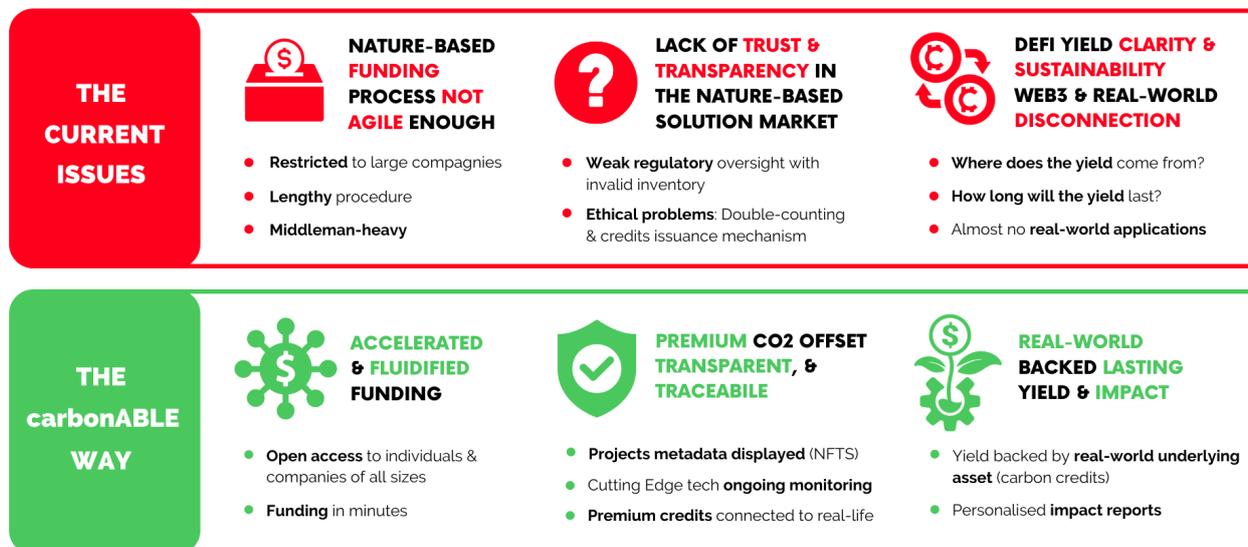
Si toutes ces initiatives s'attaquent à la dimension financière des places de marché carbone, d'autres visent à **rendre accessible au plus grand nombre l'accès aux marchés volontaires de carbone** tout en permettant aux entreprises de **vérifier l'impact des projets financés par les crédits**, cet aspect faisant régulièrement l'objet de critiques. C'est notamment l'ambition de **CarbonABLE**, créé à Grenoble en France en novembre 2021 ou encore du **Cambridge Centre for Carbon Credits (4C)**, créé au sein de l'Université de Cambridge en Angleterre, à la même date.

CarbonABLE allie NFT* et Finance décentralisée pour financer des « puits de carbone », des projets environnementaux capables de capturer et de séquestrer du carbone. CarbonABLE est construit sur la blockchain Cosmos (Atom), notamment parce qu'elle utilise un mécanisme de consensus basé sur la preuve de détention*, peu énergivore. Les projets de décarbonation³⁰ sont proposés sur la plateforme CarbonABLE et financés sous la forme de vente de NFT*, du fait de leur caractère non-fongible. Une fois financé, CarbonABLE reçoit au bout de 6 mois les premiers crédits carbone correspondants au projet.

28 « Enter : KlimaDAO », KlimaDAO, retrieved May 16, 2022, <https://docs.klimadao.finance/#8b79>

29 « A blueprint for scaling voluntary carbon markets to meet the climate challenge », Christopher Blaufelder, Cindy Levy, Peter Mannion, and Dickon Pinner, McKinsey, January 29, 2021, <https://www.mckinsey.com/business-functions/sustainability/our-insights/a-blueprint-for-scaling-voluntary-carbon-markets-to-meet-the-climate-challenge>

30 Décarbonation : *ensemble des mesures et des techniques permettant de réduire les émissions de dioxyde de carbone*. Vocabulaire de l'environnement : climat-carbone, Journal Officiel de la République française, 24 septembre 2019, https://www.connaissancedesenergies.org/sites/default/files/pdf-actualites/joe_20190924_0222_0049.pdf



CarbonABLE Lite Paper, Source, CarbonABLE : <https://carbonable.notion.site/carbonable/CarbonABLE-Lite-Paper-82bda161f3594964931b2be7d84429ff#7cb3ab5a31fc492e8333c2d2efb786ec>

Les détenteurs de NFT* obtiennent alors un rendement financier en crypto-actifs stables* et en CARBZ, un token de gouvernance et d'augmentation de rendement (*Yield*). Les projets financés par l'intermédiaire de CarbonABLE sont suivis en temps réel par Wild Sense³¹, créée avec le soutien de l'Agence spatiale européenne, et dont l'objet est de sélectionner, certifier, surveiller et garantir les projets de crédit carbone. Une première vente de NFT* en mai 2022 vise à planter « 8 000 espèces natives sur 4 hectares dans le but de connecter différentes parties de la réserve du Golfo Dulce dans le sud du Costa Rica³² » a été lancée avec succès³³.

Une dizaine de projets de décarbonation répartis sur quatre continents sont en phase de financement, ce qui représente près d'un million de tonnes de crédits CO². CarbonABLE souhaite ainsi répondre à plusieurs critiques émises à l'encontre des marchés carbone.

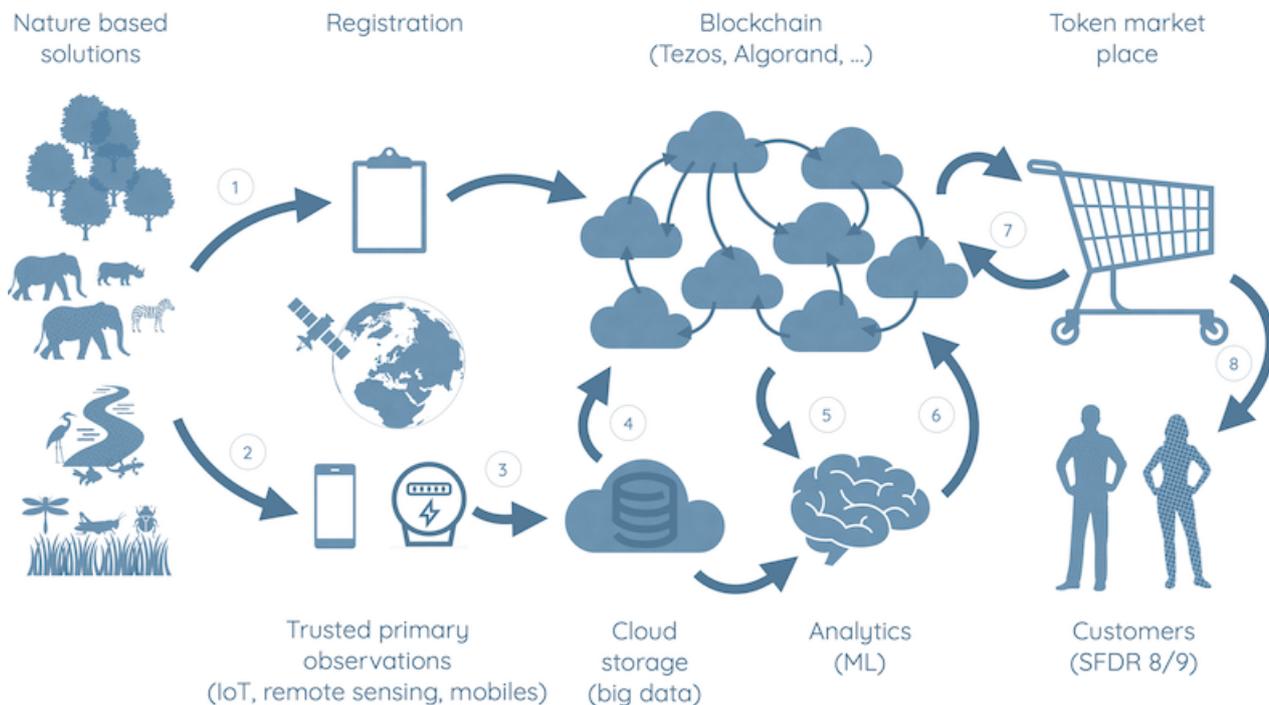
Le Cambridge Centre for Carbon Credits (4C) a pour ambition de créer « *une place de marché décentralisée de confiance où les acheteurs de crédits carbone peuvent financer directement et en toute confiance des projets respectueux de la nature* »³⁴. Cette plateforme, en cours de développement, s'appuiera sur la blockchain publique Tezos pour relier des entreprises qui financent des

31 Wild Sense: <https://www.wildsense.co/>

32 Wild Sense, Costa Rica Banegas: <https://www.wildsense.co/projects>

33 « CarbonABLE's First Mint: 160 NFTs restoring the forest at Banegas Farm! », CarbonABLE, May 3, 2022, <https://carbonable.medium.com/banegas-farm-reforesting-to-be-finance-by-carbonables-160-nfts-b4b36b5a4645>

34 « Learn about our approach and first prototype », Cambridge Center for Carbon Credit, retrieved May 16,



How the decentralised marketplace for nature-based solutions works

Source : Cambridge Centre for Carbon Credit,
retrieved May 16, 2022, <https://4c.cst.cam.ac.uk/about/marketplace>

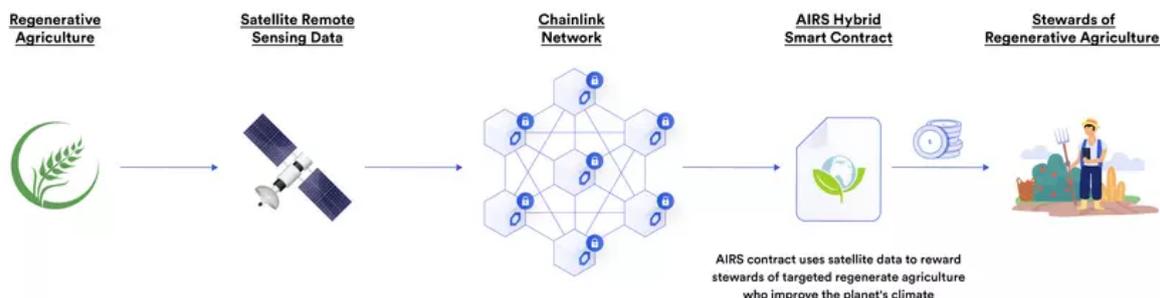
projets de compensation carbone avec des porteurs de projets de défense de l'environnement, notamment par le biais d'oracles décentralisés*, automatisés et transparents, relevant de l'imagerie satellitaire. Selon le Cambridge Centre for Carbon Credits « *le système algorithmique est capable non seulement de quantifier rétrospectivement les externalités positives qui découlent des zones de projet, mais aussi de prédire leur potentiel* », l'un des points faibles des standards classiques de certification des réductions d'émissions de carbone.

A côté d'une offre de compensation carbone destinée aux entreprises, un certain nombre de projets blockchain proposent également aux particuliers

de compenser leurs émissions de gaz à effet de serre. Comme **Dovu**, créé en 2016 à Wales en Angleterre, **Choose**, créé en 2017 à Oslo en Norvège ou encore, aux Etats-Unis, **Climate Futures** en 2018 et **Flow Carbon** en 2021. Ces services – parfois confus sur la manière dont ils procèdent – promettent à un particulier de calculer et de compenser son empreinte carbone en choisissant un projet à financer. Ces crédits carbone, tokenisés, proviennent souvent des registres classiques de type Verra ou Gold Standard.

Une autre manière de lutter contre le réchauffement climatique passe par des projets de reforestation comme ceux portés par **Open Forest Protocol**,

2022, <https://4c.cst.cam.ac.uk/>



ChainLink Labs Blockchain can help us beat climate change. Here's how.

Source : Adelyn Zhou, WeForum, Jun 30 2021,

<https://www.weforum.org/agenda/2021/06/blockchain-can-help-us-beat-climate-change-heres-how/>

GainForest ou encore le programme mené conjointement par **Green World Campaign**, l'université de **Cornwell** avec le soutien de l'oracle décentralisé **ChainLink**.

Fondé en 2020 à Genève, **Open Forest Protocol** vise à « mesurer, vérifier et financer de manière transparente des projets d'agroforesterie grâce à la technologie blockchain ». Vingt-sept projets de reboisement sont actuellement en cours au Kenya, au Costa Rica, au Panama, en Colombie et en Corée du Sud. Le plus récent, amorcé en 2022 avec la Côte d'Ivoire, implique les communautés locales et une organisation non gouvernementale pour reboiser et restaurer plus de 5 000 hectares de terres forestières dégradées dans la région de Gorké³⁵.

Open Forest Protocol est une application décentralisée (dApp*) construite sur le protocole NEAR³⁶, un protocole blockchain qui permet le développement de *smart contracts**, interopérables avec la blockchain Ethereum. Le mécanisme de consensus du protocole NEAR repose sur la preuve d'enjeu déléguée* (*delegated proof of stake*) qui utilise le *sharding*, c'est-à-dire le partitionnement d'une base de données afin de réduire le risque de centralisation des réseaux et d'offrir des transactions plus rapides et moins onéreuses.

Pour tenir compte de la nature géospatiale du reboisement, l'application décentralisée génère des jetons non fongibles (NFT*) qui représentent une zone au sein de laquelle un projet de reboisement est en cours. Alors que les informations du projet de reboisement sont stockées sur IPFS³⁷, un système

35 « Open Forest Protocol tackles climate change naturally », Julie Mollins, ForestNews, April 18, 2022, <https://forestsnews.cifor.org/76905/blockchain-platform-offers-reforestation-efforts-access-to-carbon-finance>

36 Lancé en 2020 par Illia Polosukhin et Alexander Skidanov, Near protocol permet le **développement d'applications décentralisées** (dApps*), qui repose sur des *smart contracts* à consensus de preuve de détention. Near Protocol a levé 533 millions de dollars depuis son lancement (Source : Crunchbase.com)

37 L'IPFS ou InterPlanetary File System est un protocole pair-à-pair (P2P) de distribution de contenu adressable



distribué pour le stockage et l'accès à des contenus distribués, les métadonnées du NFT* sont mises à jour « *de sorte que toutes les informations relatives au projet de reboisement sont totalement transparentes et traçables pendant toute la durée de vie du projet* » et pourront éventuellement permettre d'émettre des crédits carbone.

La plupart des projets de reboisement visent à mettre en relation des communautés locales avec des organisations de validation, ainsi que des partenaires financiers et des entrepreneurs au sein d'une même communauté décentralisée. Mais Open Forest Protocol met également en œuvre des outils de Mesure, Rapport et Vérification (MRV) parmi lesquels l'imagerie satellitaire, l'intelligence artificielle et des capteurs des l'Internet des objets (IoT), afin de certifier ou non l'avancée des projets.

Une autre initiative de reboisement est menée par **Green World Campaign**, une association américaine, en partenariat avec l'**Université de Cornwell** avec le soutien de l'oracle décentralisé* **ChainLink**. Depuis 2012, **Green World Campaign** est engagée au Kenya, en Inde, en Éthiopie et au Mexique sur des projets d'agroécologie, combinant le reboisement d'arbres et d'autres

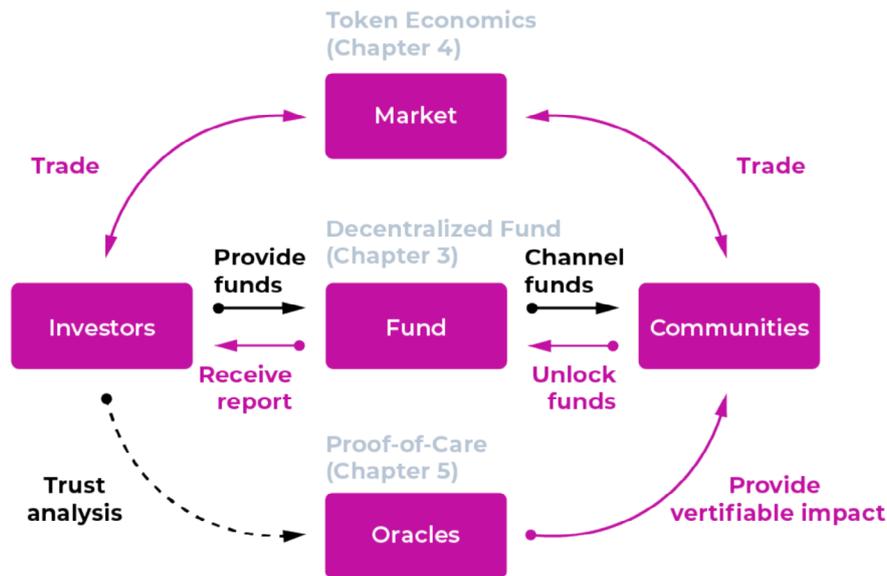
plantations. Au Kenya, **Green World Campaign** a déjà planté « *3,75 millions d'arbres, établi 100 programmes d'éco-écoles et assuré la formation des agriculteurs, la santé des femmes et des enfants et les moyens de subsistance en milieu rural*³⁸ ». En 2021, des *smart contracts** ont été développés pour récompenser automatiquement les personnes qui régénèrent des parcelles de terre en augmentant la couverture végétale, en améliorant le sol et en mettant en œuvre d'autres pratiques agricoles réparatrices, identifiées *via* les données satellitaires.

« *Lorsque les oracles de Chainlink apportent la preuve de l'amélioration d'une terre (via l'imagerie satellite) sur la blockchain, le smart contract* déclenche le versement d'une somme d'argent. Grâce à ce système, les intendants des terres peuvent recevoir rapidement et efficacement leurs récompenses. En même temps, seuls ceux qui ont un impact réel peuvent obtenir des récompenses, car le paiement n'intervient que lorsqu'une condition du monde réel est remplie et vérifiée sur la blockchain. L'ensemble de ce processus est automatisé, évolutif et à l'épreuve des fraudes, et peut être reproduit dans des centaines de cas d'utilisation dans tous les secteurs*³⁹ » explique Adelyn Zhou de Chainlink Labs.

par hypermédia. Il permet de « stocker » des fichiers ou des arborescences de fichiers de manière décentralisée et permanente, et d'y accéder via un nœud ipfs ou via un navigateur web. Il permet aussi d'héberger un site web statistique. Voir Chapitre « Contenus numériques et arts ».

38 « We All have the power to regreen the world » Greenworld, retrieved May 16, 2022, <http://greenworld.org/>

39 « How will blockchain technology help fight climate change ? Experts answer », Max Yakubowski, CoinTelegraph, September 5, 2021 <https://cointelegraph.com/explained/how-will-blockchain-technology-help-fight-climate-change-experts-answer>



Vue d'ensemble de tous les acteurs et modules impliqués dans la plateforme Gain-Forest. Les transactions permettent de lever des fonds (en noir) ou sont des incitations basées sur des tokens (en violet). *Source* : « GainForest White Paper.Version 1.5.0 », GainForest Non-Profit, retrieved May 16 2022, https://drive.google.com/file/d/1k7V8g2eHDgDSw_kttObaOy5lrksnuHal/view

Quant à **GainForest**, qui remporté le concours Hack4Climate de la COP 23 des Nations unies en 2017 et a officiellement été créé deux plus tard à Zurich, le projet se présente comme « *un fonds décentralisé utilisant l'intelligence artificielle pour mesurer et récompenser la gestion durable de la nature*⁴⁰ ». Il est construit sur la blockchain **Solana**, en raison de sa faible empreinte carbone. Le projet collecte des dons en crypto-actifs pour « *acheter des forêts à des propriétaires terriens, agrandir des parcs nationaux et prévenir la déforestation*⁴¹ ». Le prix d'un hectare de forêt tropicale vierge au Paraguay, par exemple, est de 300 dollars. Les donateurs reçoivent des informations et des photos sur le

projet qu'ils ont financé sous la forme de jetons non fongibles (NFT) que Gain Forest appelle NFTrees. Le projet combine des *smart contracts** construits sur **Solana**. Le système de Mesure, Rapport et Vérification (MRV) s'appuie sur des images satellites couplées à des photographies prises par drone et un traitement de données basé sur des algorithmes d'intelligence artificielle. Depuis le début de l'année 2022, GainForest travaille avec le ministère de l'Environnement du Paraguay pour protéger plusieurs milliers d'hectares de forêt tropicale dans le *Gran Chaco Americano* du Paraguay. C'est l'une des zones les plus vulnérables au changement climatique, et l'un des principaux puits

40 « A crypto-currency to reverse deforestation », GainForest, retrieved May 16 2022, <https://www.gainforest.net/>

41 *Ibid.*



de carbone de la planète⁴². Il s'étend en partie sur les territoires de l'Argentine, de la Bolivie, du Brésil et du Paraguay, entre les rivières Paraguay et Paraná à l'est, et l'Altiplano andin à l'ouest.

Pollution et déchets

Regen Ledger, créé en 2017 aux Etats-Unis dans l'Etat du Delaware, est une blockchain publique à preuve d'enjeu* (PoS), développée avec le SDK* **Cosmos** et conçue « *pour la vérification des revendications, des accords et des données relatives à l'état écologique*⁴³ ». Regen Network fournit une plateforme ouverte conçue spécifiquement pour faire fonctionner diverses applications « *telles que les crédits carbone régénératifs*⁴⁴, *la transparence de la chaîne d'approvisionnement, le suivi de la reforestation et les véhicules d'investissement tels que les obligations écologiques*⁴⁵ ».

Le livre blanc de Regen Network, mis à jour le 15 février 2021⁴⁶, propose « *la création d'un système décentralisé permettant de surveiller et de vérifier l'état écologique et le changement d'état [des lieux], (...)*

pour créer un grand livre comptable écologique capable de récompenser la régénération écologique par le biais de contrats intelligents ». La proposition de Regen Network est de « *récompenser la régénération écologique* » par le biais de *smart contracts*^{*47}.

L'architecture de la blockchain Regen Ledger articule trois concepts pour relier l'état écologique d'un lieu avec un financement participatif :

- Les *Ecological State Protocols* (ESPs), qui définissent, *via* des algorithmes, les conditions nécessaires à la vérification du changement d'état sur une parcelle.
- Les *Supply Protocols* (SPs) qui permettent de lier l'état écologique aux chaînes d'approvisionnement de manière fiable.
- Les *Ecological Contracts* (ECs) qui permettent le financement et la rémunération suite au changement d'état.

42 « Solana-Based Climate Change Project Employs 'NFTrees' to Save Rainforests », Ian Allison, Coindesk, April 21, 2022, <https://www.coindesk.com/business/2022/04/21/solana-based-climate-change-project-employs-nftrees-to-save-rainforests/>

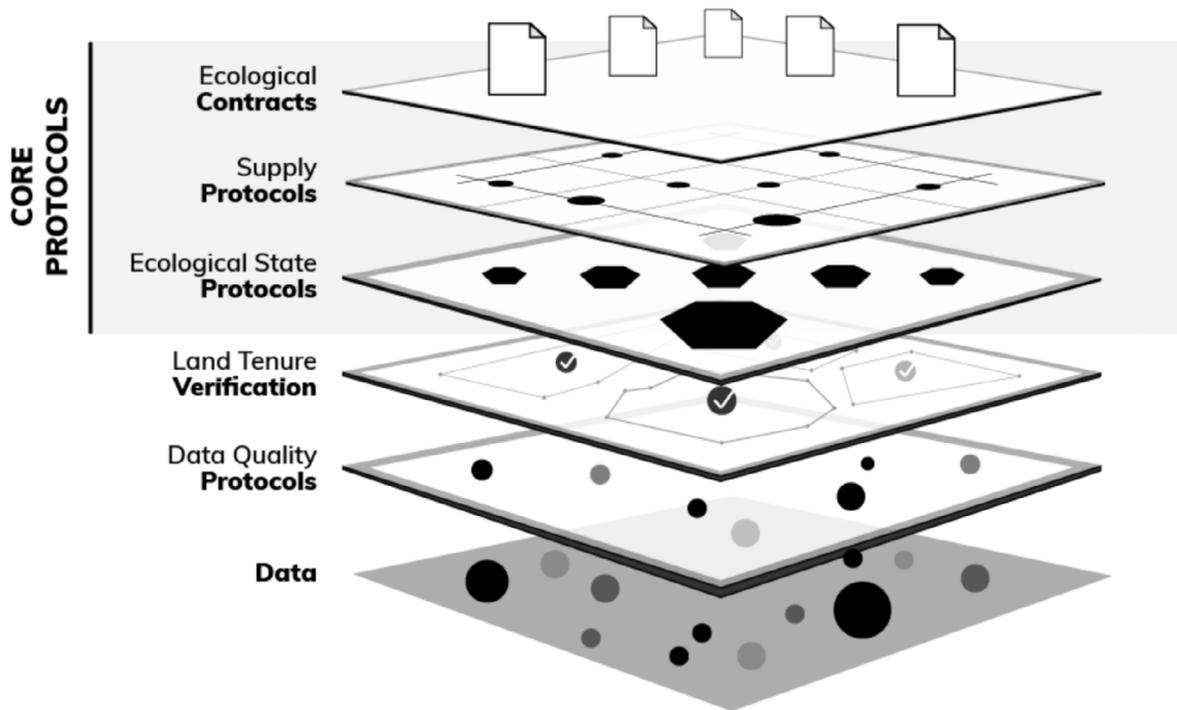
43 « Our Approach », Regen Network, retrieved May 16, 2022, <https://www.regen.network/developers/>

44 En travaillant notamment avec American Carbon Registry, Verra et Gold Standard

45 « Regen Network Development, Inc », LinkedIn, retrieved May 16, 2022, <https://www.linkedin.com/company/regen-network/about/>

46 « Regen Network Whitepaper. Version 1.3 », G. Booman, A. Craelius, B. Deriemaeker, G. Landua, W. Szal, B. Weinberg, Regen Network, February 15, 2021, <https://regen-network.gitlab.io/whitepaper/WhitePaper.pdf>

47 « Regen Network Economics Technical Paper An Ecological Market-Commons, Secured by Proof-of-Stake. Version 0.2 », G. Landua, K. Birchard, W. Szal, Regen Network, February 16, 2021, <https://regen-network.gitlab.io/whitepaper/Economics.pdf>



How Regen is Creating an Eco-Friendly Blockchain

Source : Regen Network, November 5, 2018, retrieved May 16 2022, <https://medium.com/regen-network/lets-cut-to-the-chase-for-all-the-great-environmental-projects-blockchain-supports-it-s-a-c3ea96401c28>

Plusieurs projets de séquestration du carbone dans le sol construits sur Regen Network ont actuellement en cours en Australie, aux Etats-Unis, en République démocratique du Congo, au Kenya, ou encore en Equateur⁴⁸. **Eco-Cacao**, une coopérative d'agriculteurs producteurs de cacao dans la province d'Esmeraldas, en Équateur gère des fermes agro forestières dans la région du Chocó-Darién, qui s'étend le long de la côte colombienne du Pacifique, du Sud-Ouest du Panama au Nord-Est de l'Équateur. Eco-Cacao vérifie la gestion durable des terres et verse une

prime aux agriculteurs qui gèrent avec succès des exploitations reproduisant la forêt native, qui génèrent ainsi des rendements élevés de séquestration du carbone tout en augmentant la biodiversité sur l'exploitation. L'état des parcelles de terres est enregistré sur la blockchain Regen Ledger afin d'en avoir une vision transparente et de procéder au paiement et financement de leur gestion écologique. Ils sont déclenchés pour l'instant par deux certificateurs tiers impliqués dans le projet : Terra Genesis International⁴⁹ et le Seed Guardian Network⁵⁰.

48 « Discover Ecocredits and NCT Basket tokens », Regen Registry, retrieved May 16, 2022, <https://registry.regen.network>

49 Tera Genesis: <https://terra-genesis.com/>

50 Seed Guardian: <https://www.gardenorganic.org.uk/seed-guardians>



Regen Network s'appuie ainsi sur une variété de sources de données pour vérifier l'état écologique des parcelles, dont notamment des données de télédétection telles que l'imagerie par satellite et par drone, des données émises par des capteurs de l'Internet des Objets (IoT), les données de Systèmes d'information géographiques (SIG) publics ou encore des données soumises par les utilisateurs eux-mêmes, telles que les résultats des analyses de sol.

Dans le domaine de la lutte contre la pollution, notamment du plastique dans les océans, **Plastic Bank**, démarré en 2013 depuis le Canada et **Ocean Plastik** créé en 2018 depuis la République Tchèque, mais dont l'activité semble être suspendue depuis l'épidémie de Covid 19, s'appuient tous deux sur un concept simple : « *nettoyer les océans en payant les gens pour collecter les déchets plastiques - ce qui génère également des revenus pour les aider à améliorer leur vie*⁵¹ ».

Plastic Bank, dont les activités de collecte de déchets ont cours actuellement au Brésil, en Indonésie, aux Philippines et en Égypte, crée des « écosystèmes de recyclage éthiques dans les communautés côtières et re-traite les matériaux pour les réintroduire dans la chaîne d'approvisionnement mondiale ».

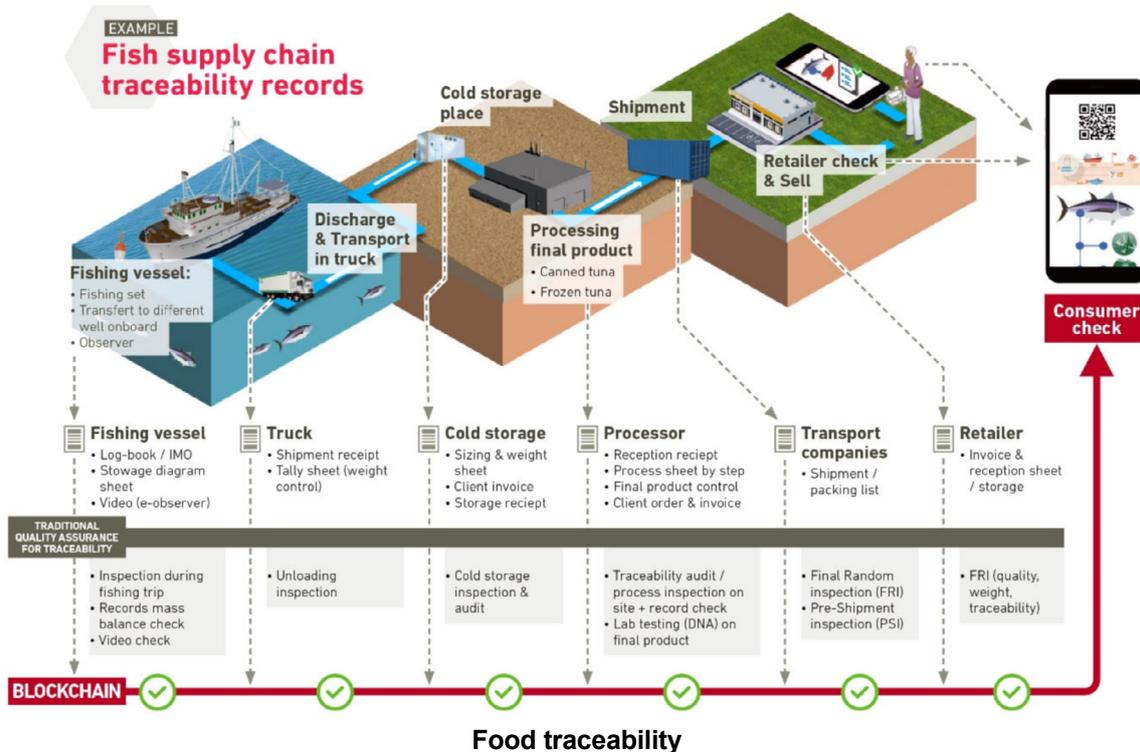
Selon Plastic Bank, l'équivalent de 41 000 tonnes de plastique auraient été collectées au 26 janvier 2022. 38 000 personnes seraient enregistrées en tant que collecteurs sur la plateforme. La collecte et le paiement du plastique récupéré leur auraient permis une augmentation de 40 % de leurs revenus. La plateforme est construite par IBM sur Hyperledger Fabric, une blockchain privée et permissionnée, nous empêchant d'avoir accès à leur données.

Quant à Ocean Plastik, il souhaite lancer RPNDEX⁵² courant 2022, une place de marché B-to-B décentralisée qui fournirait aux entreprises de recyclage et aux fabricants de plastique une plateforme unique pour acheter et vendre des granulés de plastique recyclé.

51 « Plastic Bank », IBM, retrieved May 16, 2022, <https://www.ibm.com/case-studies/plastic-bank-systems-linuxone>

52 « Decentralized Marketplace for recycled plastic materials », RPNDEX, retrieved May 16, 2022, <https://www.rpndex.com/>

Seafood supply chain traceability from traditional records to blockchain



Food traceability

Source : Bureau Veritas. White Paper (2017) in Blaha, F. & Katafano, K. 2020. « Blockchain application in seafood value chains ». FAO Fisheries and Aquaculture Circular No. 1207. Rome, FAO. <https://doi.org/10.4060/ca8751en> <https://www.fao.org/3/ca8751en/ca8751en.pdf>

Vie aquatique

La pêche et les produits de la pêche font partie, selon l'Organisation des Nations unies pour l'alimentation et l'agriculture (FAO) « des denrées alimentaires les plus échangées dans le monde, avec en 2016, environ 35 % de la production mondiale de poisson qui a fait l'objet d'un commerce international⁵³ », dont 60% de la quantité totale provient de pays en développement. Comment s'assurer que les opérations de pêche n'épuisent pas les ressources naturelles ? L'Objectif de

développement durable 14 vise d'ailleurs à offrir « un cadre permettant de gérer durablement les écosystèmes marins et côtiers et les protéger des effets résultats des activités humaines⁵⁴ ».

Plusieurs initiatives blockchain relèvent du domaine de la traçabilité de la chaîne de valeur des produits de la pêche, parmi lesquelles **Provenance** en Indonésie depuis 2016, **WWF-New Zealand**, **Consensys**, **Sea Quest**, **TraSeable Solutions** aux Îles Fidji en 2017, **Pacifical**, **Atato Pacific** en 2018,

53 « Blockchain Application in seafood value chains », Francisco Blaha, Kenneth Katafano, FAO, 2020, <https://www.fao.org/3/ca8751en/CA8751EN.pdf>

54 Objectif de développement durable 14 : Conserver et exploiter de manière durable les océans, les mers et les ressources marines aux fins du développement durable <https://www.un.org/sustainabledevelopment/fr/oceans/>



OpenSC, WWF- Australia, BCG Digital Ventures Australia en 2019, Bumble Bee Foods en mars 2019, Fishcoin en 2018, Sustainable Shrimp Partnership en Equateur en mai 2019. La totalité de ces expérimentations assure la traçabilité du thon *via* une blockchain privée, sauf **Pacifical qui a développé une plateforme sur la blockchain Ethereum**. La promesse de ces initiatives est résumée par le Bureau Veritas à travers le schéma en page précédente.

Le chapitre « Agriculture et alimentation » est consacré à la traçabilité alimentaire et la traçabilité des produits de la pêche.

Eau et assainissement

Parce que 2,2 milliards de personnes n'ont pas accès à une eau potable gérée de manière sûre, et plus de 4,2 milliards de personnes n'ont pas accès à un système d'assainissement, l'Objectif de développement durable 6 vise « *l'accès universel et équitable à l'eau potable, à l'hygiène et à l'assainissement d'ici 2030, en particulier pour les populations vulnérables. Il appelle également à une gestion durable de cette ressource, et mentionne la réduction du nombre de personnes souffrant de la rareté de l'eau. Cet objectif intègre la notion de gestion transfrontalière de cette ressource, essentielle à la gestion durable mais aussi favorable à la paix et à la coopération*⁵⁵ ».

Selon Therese Flapper, *associate principal - Infrastructure and Water* chez Arup, bureau d'études et de conseil en ingénierie britannique, « *les blockchains sont une technologie idéale pour suivre les transactions et les activités de mise en conformité dans le domaine de l'eau. Les régulateurs, les utilisateurs d'eau et toutes les parties prenantes disposent de la même copie des informations relatives aux transactions et à la conformité de l'eau sur l'ensemble d'un réseau d'eau, sans aucune divergence*⁵⁶ ».

Plusieurs initiatives blockchain sont en cours d'expérimentation dans le domaine de l'assainissement et de la gestion

⁵⁵ Objectif de développement durable 6 - Garantir l'accès de tous à l'eau et à l'assainissement et assurer une gestion durable des ressources en eau, <https://www.agenda-2030.fr/17-objectifs-de-developpement-durable/article/odd6-garantir-l-acces-de-tous-a-l-eau-et-a-l-assainissement-et-assurer-une>

⁵⁶ « Blockchain and the built environment.Version 1.2 », ARUP, February 2019, <https://www.arup.com/>

de l'eau, pour notamment remettre en question les systèmes centralisés détenus et gérés par une seule entité, qu'elle soit privée ou publique, ou remédier à la complexité des marchés de l'eau reposant sur de trop nombreux intermédiaires. D'autres initiatives fléchissent les investissements en crypto-actifs vers des projets de gestion de l'eau.

Le marché de l'eau implique souvent de nombreux intermédiaires. D'où cette idée de mettre en place des *smart contracts** afin de gérer de manière rapide l'approvisionnement, la livraison et la facturation de l'eau, y compris dans un contexte changeant, par exemple en cas de sécheresse. Les promoteurs de ces initiatives mettent en avant la transparence de la production et des transactions pour tous les utilisateurs d'un réseau d'eau. Cela favorise l'engagement et la responsabilité des parties prenantes, tout en permettant de se passer d'un certain nombre d'intermédiaires, ou tout du moins d'automatiser de nombreux processus manuels particulièrement chronophages.

Le cas de l'Australie illustre les problématiques que rencontrent les marchés d'échange de l'eau dès lors qu'ils sont gérés de manière relativement opaque.

Le marché d'échange d'eau le plus actif en Australie est celui du marché du bassin de Murray-Darling (MDB), où 97 % de tous les échanges d'allocations et 77 % des échanges de droits sont effectués⁵⁷. A chaque sécheresse, ce marché est notamment critiqué « *pour son manque d'information sur qui négocie quelles ressources et qui bénéficie finalement de ces échanges*⁵⁸ ».

En 2020, **Civic Ledger** a collaboré avec l'agence gouvernementale Cooperative Research Centre for Developing Northern Australia (CRCNA) pour tester la tenue du système d'approvisionnement en eau de Mareeba-Dimbulah dans l'extrême nord du Queensland sur une blockchain publique. Dans cette seule région, il existe « *neuf textes législatifs et plans opérationnels qui régissent le commerce de l'eau, de multiples agences qui réglementent et exploitent le réseau d'eau, et 2 000 utilisateurs d'eau*⁵⁹ ». **Water Ledger** a été construit sur la blockchain Ethereum et utilise la norme ERC 1753 - *Smart Contract Interface for Licences*⁶⁰ afin de gérer la délivrance de licences et de permis, jusqu'alors entièrement manuelle, s'appuyant sur du papier et disséminée entre de multiples entités. Ces licences ont été dématérialisées sous la forme de *smart contracts** permettant à chacun d'interagir au sein d'un marché pair-

57 « Member Spotlight: Civic Ledger, Digitally Transforming Water », June 10, 2020 Fintech Australia Newsroom Spotlight <https://www.fintechaustralia.org.au/member-spotlight-civic-ledger-digitally-transforming-water/>

58 « Blockchain and the Built Environment », February 2019 Version 1.2, <https://www.arup.com/>

59 « How distributed ledger technology is revolutionizing water markets », Katrina Donaghy, Fraser MacLeod, WeForum, June 22, 2021, <https://www.weforum.org/agenda/2021/06/distributed-ledger-technology-water-markets>

60 « EIP-1753: Smart Contract Interface for Licences », Ethereum Improvement proposals, retrieved May 16,



à-pair d'échange de l'eau. Le délai de réalisation d'une transaction est ainsi passé de 90 jours à moins de 7 jours après la mise en place de Water Ledger.

De plus, en utilisant la norme ERC 1753⁶¹ pour les *smart contracts**, les règles d'affectation de l'eau, lorsqu'elle

vient notamment à manquer, peuvent être mises à jour en temps réel par les autorités publiques pour « *l'affecter en priorité à un usage domestique*⁶² » explique Katrina Donaghy, CEO de Civic Ledger.

2022, <https://eips.ethereum.org/EIPS/eip-1753>

61 Cette proposition d'amélioration d'Ethereum (Ethereum Improvement Proposal - EIP) propose une norme Ethereum pour la délivrance de licences, permis et subventions (Licences), <https://eips.ethereum.org/EIPS/eip-1753>

62 « How distributed ledger technology is revolutionizing water markets », Katrina Donaghy, Fraser MacLeod, WeForum, June 22, 2021, <https://www.weforum.org/agenda/2021/06/distributed-ledger-technology-water-markets>

ENJEUX ET QUESTIONS

Quelque 63 initiatives actives à ce jour s'inscrivent explicitement dans la lutte contre le réchauffement climatique et la préservation de l'environnement. C'est dire si s'intéresser aux blockchains et à l'environnement n'est pas un oxymore. Le mécanisme de consensus de la preuve de travail*, utilisé par les blockchains de première génération comme Bitcoin ou Ethereum, repose sur une dépense énergétique afin de sécuriser les transactions sur le réseau.

Des initiatives blockchain, comme **Toucan Protocol** ou **KlimaDAO** viennent ainsi fluidifier les **marchés volontaires de carbone traditionnels** qui font l'objet d'un certain nombre de critiques^{1,2}. En effet, les émetteurs de crédits

carbone, comme Verra ou Gold Standard, n'offriraient pas de méthodologie suffisamment robuste pour démontrer sans ambiguïté l'impact réel des projets leur permettant de générer des crédits carbone. La pérennité de projets de séquestration de carbone sur de longues périodes, allant parfois jusqu'à vingt ans³ fait également l'objet de critiques.

Par exemple, les réductions des émissions dues à la déforestation et à la dégradation REDD et REDD+ ont été inventées et lancées en 2011, sous l'impulsion de l'ONU, pour financer des projets de conservation dans les pays en développement, dans le but d'atténuer le changement climatique⁴. Or, comme l'explique Greenpeace « *les programmes de déforestation*

1 « Carbon offsets used by major airlines based on flawed system, warn experts », Patrick Greenfield, May 4, 2021, <https://www.theguardian.com/environment/2021/may/04/carbon-offsets-used-by-major-airlines-based-on-flawed-system-warn-experts>

2 « Carbon offsets are going primetime and they're not ready » Tim McDonnell, May 20, 2021, <https://qz.com/2009746/not-all-carbon-offsets-are-a-scam-but-many-still-are/>

3 « How our partner Wildsense monitors carbon sink restoration from space », CarbonABLE, June 3, 2022, <https://carbonable.medium.com/how-our-partner-wildsense-monitors-carbon-sink-restoration-from-space-86e3a4ca759>

4 REDD+ s'appuie sur des approches politiques et un système de mesures d'incitation positives pour réduire les émissions provenant de la déforestation et de la dégradation (REDD) et pour aider à la conservation des stocks existants de carbone forestier, à la gestion forestière durable et à l'accroissement des stocks de carbone forestier (+) dans les pays en voie de développement. Source : Interactions FLEGT-REDD+ Note d'information n°2 Janvier 2011. Proforest avec les contributions de représentants officiels de la Commission européenne et des Etats membres, du gouvernement de Norvège et des représentants de FCPF et de l'ONU- REDD. <https://europa.eu/capacity4dev/file/10546/download?token=RvEfqdVx>



évitée génèrent et vendent des crédits carbone en fonction de la quantité de déforestation qu'ils prétendent empêcher. Pour calculer ces économies de carbone, ils essaient de prédire l'ampleur de la déforestation qui aurait lieu si le projet n'existait pas⁵ ». Ces calculs hypothétiques s'avèrent très fragiles dès lors qu'il s'agit de vérifier sur le terrain la véracité de ces compensations carbone.

Or les crédits carbone sont entre-temps générés et vendus à des entreprises, ce qui remet en cause l'efficacité même de ce type de mécanisme. L'analyse la plus récente en la matière, menée par Unearthed, la branche investigation de Greenpeace, accompagnée du média anglais *The Guardian* et de l'ONG allemande SourceMaterial ont analysé en 2021 « dix projets de compensation de la déforestation réduite sur lesquels s'appuient les grandes compagnies aériennes dans le cadre de leurs engagements de réduction des émissions et qui sont certifiés par Verra, le plus grand émetteur de crédits carbone au monde⁶ », en s'appuyant notamment sur l'analyse d'experts,

de la documentation des projets et sur l'analyse par satellite de la déforestation dans et autour des projets soutenus par British Airways, easyJet et United Airlines. Et leur verdict est pour le moins très mitigé⁷.

Si l'intérêt de tokeniser des crédits carbone à partir des registres internationaux de type Verra ou Gold Standard est de les inclure dans la Finance décentralisée, certains projets blockchains, comme **Nori**, visent à vérifier de manière plus fine, sur le terrain, l'efficacité de ces derniers, notamment par l'utilisation d'oracle décentralisé comme **Chainlink**.

La promesse de ces initiatives concerne les activités d'agriculture régénératrice, de reboisement ou encore de reforestation, comme **Open Forest Protocol**, **GainForest** ou **Eco-Cacao via Regen Network**, sûrement plus simple à mesurer et à quantifier que des projets d'évitement de déforestation. Ces projets s'inscrivent dans la continuité du marché du carbone et ne sont donc pas exempts des critiques émises à l'encontre de ces mécanismes financiers.

5 « Top airlines' promises to offset flights rely on 'phantom credits' », Joe Sandler Clarke, Luke Barratt, May, 4, 2021, <https://unearthed.greenpeace.org/2021/05/04/carbon-offsetting-british-airways-easyjet-verra/>

6 Ibid.

7 Ibid.

L'usage de registres distribués et publics pourrait-il véritablement améliorer les déficiences des marchés carbone ?

D'autres projets, notamment liés au marché de l'eau comme en Australie, démontrent en revanche l'efficacité de la mise en place d'un registre distribué sur un marché complexe réunissant de nombreux participants. Il apporte plus de transparence, supprime des intermédiaires et fluidifie les échanges. Les initiatives menées dans le domaine des services publics (Voir Chapitre Gouvernement et démocratie) fonctionnent sur le même schéma

Encore une fois, il ne s'agit pas de rajouter une dimension blockchain à des projets pour qu'il gagnent en efficacité mais de s'interroger

sur la manière dont l'usage d'un registre commun permet de pallier à l'asymétrie d'information entre les différents acteurs de chaînes de valeur complexes.

Comme les blockchains sont un outil dont l'intérêt ne dépend que de l'usage qui en est fait, aucun de ces projets ne peut garantir la véracité et l'exactitude des informations partagées dans un registre distribué.

De cet écueil, tenant à la qualité des données, découle l'intérêt ou l'inutilité de ces projets dont le manque de maturité ne nous permet pas encore de dire s'ils versent dans un nouveau « *greenwashing* » ou bien sont les prémices de changements plus profonds participant à la résilience climatique.

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 Antonopoulos¹, 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 Raspberry 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



Les contenus de ce rapport sont mis à disposition selon les termes de la **Licence Creative Commons : Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International**.

Vous êtes autorisés à : Partager — copier, distribuer et communiquer le rapport par tous moyens et sous tous formats. Adapter — remixer, transformer et créer à partir du rapport selon les conditions suivantes : Attribution — Vous devez créditer le rapport, intégrer un lien vers la licence et indiquer si des modifications au rapport ont été effectuées. Vous devez indiquer ces informations par tous les moyens raisonnables, sans toutefois suggérer que l'Offrant vous soutient ou soutient la façon dont vous avez utilisé son rapport. Pas d'Utilisation Commerciale — Vous n'êtes pas autorisés à faire un usage commercial de ce rapport, tout ou partie du matériel le composant. Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant le rapport original, vous devez diffuser le rapport modifié dans les mêmes conditions, c'est à dire avec la même licence avec laquelle le rapport original a été diffusé. V.1.0