



WEB 3.0, ARTS & SCIENCES

SEPTEMBRE 2022

WWW.BLOCKCHAINFORGOOD.FR



BLOCKCHAIN
@POLYTECHNIQUE

bpifrance
SERVIR L'AVENIR



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 WEB 3.0, ARTS ET SCIENCES

[Noémie Dié](#), [Alejandro Gómez](#), [Audran Gouis](#), [Ani Ramos](#).

TABLE DES MATIÈRES

ENCADRÉ : LIRE, ÉCRIRE, DÉTENIR : DU WEB STATIQUE AU WEB DÉCENTRALISÉ -----	8
CONTENUS / DONNÉES / INDEX DÉCENTRALISÉS -----	11
HÉBERGEMENT DÉCENTRALISÉ DE DAPPS ET DE NŒUDS BLOCKCHAIN -----	12
MÉDIA ET JOURNALISME -----	16
RÉSEAUX & MÉDIAS SOCIAUX -----	17
ARTS, MUSIQUE & VIDÉO -----	20
ENCADRÉ : COMMENT FONCTIONNE UN NFT ? -----	21
SCIENCE DÉCENTRALISÉE -----	28
ENJEUX ET QUESTIONS -----	31
GLOSSAIRE -----	32
ÉDITEUR -----	42



WEB 3.0, ARTS & SCIENCES

Nombre de projets dans la base : 75

Nombre de projets actifs : 46

Nom des projets actifs : Akasha World ; Arweave ; Binded ; Bittunes ; Blockchain My Art ; BlockchainyourIP ; Brave (Basic Attention) ; Breaker ; Bridgit ; CyberFM Mainstream For The Underground ; Decent ; DTube ; eyeWitness to Atrocities ; Fiducia ; FilmChain ; Gab ; Golem ; Gridcoin ; HashingDNA ; Inflow Music ; Klapcoin ; Lucidity ; Lympo.io ; MAP ; Mediachain ; Minds ; Monegraph ; Opus ; Peertracks ; PubliQ ; Resonate ; Royal ; Sapien ; Sia (ou Skynet) ; Steem ; Storj ; The Safe Network ; Tokit (Breaker) ; Torum ; Truepic ; Unbiased ; URights ; Vevue ; Vezt ; VitaDAO ; ZeroNet ; *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/>

Si le web permet d'échanger des informations et des contenus, les blockchains publiques permettent d'échanger de la valeur. Mais, qu'en est-il de l'impact des blockchains sur ces mêmes contenus, qu'ils soient artistiques, culturels, scientifiques ou encore produits par des journalistes ? Quel est l'impact du caractère décentralisé des blockchains publiques sur les applications développées au sein de ces nouveaux écosystèmes ?

Des initiatives blockchains viennent bousculer la structure actuelle du web, le stockage et le partage de données ou d'applications mais également la manière dont la valeur circule lorsqu'elle est attachée à des contenus numériques.

Avec en paragon, la vague des jetons non fongibles* (NFT) depuis 2021, consistant à enregistrer dans une blockchain publique un certificat d'authenticité. Ce caractère distribué propre aux blockchains publiques est aussi l'occasion d'interroger la manière dont l'information circule entre des infrastructures centralisées et décentralisées : hébergement et stockage distribués, salles de rédaction, journalisme et médias sociaux décentralisés, contenus numériques dont notamment la musique et les vidéos dont la propriété et les droits d'auteurs sont dorénavant programmables et enfin Sciences décentralisées (DeSci), ce mouvement qui augure une remise en question de la concentration opérée par une poignée d'intermédiaires dans le domaine des publications scientifiques.

Ces projets blockchains initient de nouveaux paradigmes de création, de financement, de monétisation et de circulation des contenus, qui tous, sont largement associés au Web dit 3.0. Tim Berners Lee en parlait dès 1994 en l'appelant Web sémantique, lorsqu'il imaginait un réseau distribué et sans autorité centrale, dont les contenus pourraient faire sens à la fois pour les gens et pour les machines¹.

Lire, écrire, détenir : du web statique au web décentralisé

Le web est l'un des services rendus possible par l'invention d'internet, un réseau de réseaux informatiques, mondial, accessible à tous et qui s'appuie sur un ensemble standardisé et ouvert de protocoles de transfert de données. Le World Wide Web, quant à lui, est un système hypertexte public fonctionnant sur le réseau Internet dont Tim Berners-Lee donne le coup d'envoi en août 1991.

Il est dorénavant courant de rendre compte de l'évolution du web en distinguant trois périodes correspondant chacune à une évolution de ses usages, les uns n'empêchant pas les autres. De manière schématique, le web 1.0 a permis aux gens de lire ; le web 2.0 permet aux gens de lire et d'écrire ; le web 3.0 permet aux gens de lire, écrire et détenir.

Le web 1.0, que le grand public découvre au milieu des années 1990, équivaut à

la publication de pages web sur des serveurs informatiques consultables à partir d'un navigateur web. Ce web est dit statique, car il reproduit la consommation des médias traditionnels de l'époque. Comme une personne lit un journal imprimé, un internaute lit, à l'écran, une page accessible *via* le web.

Le web 2.0, également appelé « web participatif », marque le moment où l'internaute, à partir des années 2000, n'est plus seulement le consommateur passif d'informations affichées sur un écran mais devient également le producteur de contenus, que ce soit sur des blogs, des wikis ou sur les premiers réseaux sociaux, au sein desquels il interagit, partage et échange des contenus de tout genre.

Cette période se caractérise tout à la fois par une large démocratisation des usages du web auprès du grand public et par la constitution des géants du numérique qui ont capitalisé sur l'augmentation exponentielle du nombre d'utilisateurs attirés par la simplicité des services proposés. Avec ce biais que, lorsque le service est accessible gratuitement, le modèle de ces plateformes repose sur l'exploitation massive des données personnelles des utilisateurs du service, la plupart du temps de manière opaque.

Les services du web 2.0, en même temps que le grand public s'en emparait, ont eu pour conséquence de centraliser les grandes applications du web entre

1 « Plenary at WWW Geneva 94 », Tim Berners Lee, 1994, w3.org, <https://www.w3.org/Talks/WWW94Tim/>



	Web 1.0	Web 2.0	Web 3.0
Interaction	Lire	Lire - Ecrire	Lire – Ecrire - Détenir
Medium	Texte statique	Contenu interactif	Economie virtuelle
Organisation	Entreprises	Plateformes	Réseaux
Infrastructure	Ordinateur personnel	Cloud et mobile	Cloud Blockchain
Contrôle	Décentralisé	Centralisé	Décentralisé

L'évolution du World wide web - Traduction : Blockchain for Good

Source : « Blockchain Won't Save the World », Anthony Day, <https://www.blockchainwontsavethe.world/about> & https://www.linkedin.com/posts/anthonijday_blockchain-technology-innovation-activity-6874640878640615424-g3nx/

les mains de quelques acteurs comme Google, Meta (Facebook, Instagram, WhatsApp), Amazon, Uber, Airbnb ou encore Blablacar. Ces géants du web ont un modèle d'affaires assimilable au capitalisme de surveillance dont la notion a été popularisée en 2014 par l'économiste américaine Shoshana Zuboff, professeure émérite à la Harvard Business School. Le capitalisme de surveillance décrit l'évolution du capitalisme industriel du 20^e siècle, emmené par le constructeur automobile Ford vers un capitalisme de données, optimisé par Google dans les années 2000. Il est fondé sur l'enregistrement systématique des données personnelles

des individus et de leurs interactions, la plupart du temps à leur insu. Ces données personnelles sont analysées à l'aide de puissants logiciels (*big data* et intelligence artificielle) afin de les vendre à des annonceurs en ligne.

Le web 3.0, ou web décentralisé, est une tentative de re-décentralisation du web², qui s'appuie largement sur les technologies de registre distribué et les blockchains publiques pour y parvenir. L'avènement d'un web décentralisé coïncide avec la volonté d'une multitude d'acteurs de se dégager du modèle d'affaires des géants du web.

2 « What is Web3 ? Here Are Some Ways To Explain It To A Friend », James Beck, January 12, 2022, <https://consensus.net/blog/blockchain-explained/what-is-web3-here-are-some-ways-to-explain-it-to-a-friend/>

Toutefois, le web 3.0 n'est pas épargné par ses détracteurs, qui dénoncent, parfois à juste titre, la création de nouvelles plateformes centralisées qui opèrent de manière structurelle des services similaires à ceux du web 2.0 ³.

«l'avènement de sociétés pacifiques et inclusives, tout en assurant l'accès de tous à la justice, et mettre en place, à tous les niveaux, des institutions efficaces et responsables ? Voici un tour d'horizon des initiatives blockchain en la matière.

Alors, qu'apportent les blockchains dans les domaines de la création, du partage et de l'exploitation des contenus numériques, que ce soit dans les domaines de l'art, la culture, le journalisme, les médias sociaux ou encore des publications scientifiques ?

En quoi les blockchains impactent-elles la création, le partage et la manière dont ces contenus sont consommés, échangés et valorisés ? Comment les blockchains peuvent aider à bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation, comme le promeut l'Objectif de développement durable 9⁴ ? Aideront-elles à ce que « *les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables* », l'Objectif de développement durable 11⁵ ?

Comment promouvoir, comme le décrit l'Objectif de développement durable 16⁶,

3 « Le "Web3" expliqué en quatre questions », Olivier Clairouin, 20 avril 2022, https://www.lemonde.fr/pixels/article/2022/04/20/le-web3-explique-en-quatre-questions_6122944_4408996.html

4 Objectif de développement durable 9 : Mettre en place une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation <https://sdgs.un.org/fr/goals/goal9>

5 Objectif de développement durable 11 : Faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables. <https://sdgs.un.org/fr/goals/goal11>

6 Objectif de développement durable 16 : Promouvoir l'avènement de sociétés pacifiques et ouvertes aux fins du développement durable. <https://sdgs.un.org/fr/goals/goal16>



Contenus / données / index décentralisés

Depuis plus d'une décennie, le développement d'une offre d'hébergement ou de *Cloud Computing* à destination des entreprises qui souhaitent externaliser la gestion des données qu'ils émettent et reçoivent représente aujourd'hui un marché de plusieurs milliards de dollars, contrôlé par une poignée d'acteurs parmi lesquels Amazon Web Services, Microsoft Azure, Google Cloud ou encore Alibaba. Cette offre de *Cloud computing*, décomposable en IaaS (*Infrastructure-as-a-Service*), PaaS (*Platform-as-a-Service*) et SaaS (*Software-as-a-Service*) selon l'étendue des données et services hébergés à distance, consiste, pour l'opérateur de *Cloud*, à assurer l'hébergement de contenus, de données et d'application dans des centres de serveurs maintenues par leurs soins.

L'InterPlanetary File System (ou IPFS, système de fichier inter-planétaire) est un système distribué de fichiers pair-à-pair dont l'objectif est de stocker des informations, comme des fichiers, des sites web, des applications ou encore données, de manière totalement décentralisée, sécurisée et confidentielle, permettant ainsi de se prémunir contre toute forme de censure. l'IPFS n'est pas une blockchain mais un système

de stockage de données parfaitement adapté aux applications blockchains qui nécessitent d'accéder à des contenus, ce qui fait dire à certains qu'IPFS est un « *disque dur pour les blockchains*⁷ ».

Plus précisément, IPFS cherche à créer un web persistant⁸ et distribué qui ne s'appuie plus sur la localisation d'un contenu mais sur le contenu en lui-même. 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 de la machine où la donnée ou encore la page est hébergée ; une recherche dans l'IPFS consiste à demander au système « le contenu que l'on recherche », identifié par un *hash* cryptographique* unique et permanent. « *De cette façon, le système tire parti de la proximité physique. Si une personne très proche de moi possède ce que je veux, je l'obtiendrai directement auprès d'elle au lieu de me connecter à un serveur central*⁹ » explique l'ingénieur Karan Kwatra.

Créé en 2014 par Juan Benet, IPFS est un protocole *open source* qui pourrait largement se développer à côté du protocole Hypertext Transfer Protocol (HTTP), inventé par Tim Berners-Lee en 1991.

7 « What is IPFS ? The hard drive for Blockchain », iCommunity, retrieved May 23, 2022, <https://icommunity.io/en/what-is-ipfs-the-hard-drive-for-blockchain/>

8 « Persistence, permanence, and pinning », IPFS doc, retrieved July 21, 2022, <https://docs.ipfs.io/concepts/persistence/#persistence-versus-permanence>

9 « What is IPFS ? », Karan Kwatra, Mar 15 2018, retrieved May 23, 2022, <https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5>

IPFS est déjà largement utilisé¹⁰, que ce soit par des initiatives blockchain ou non, dans des secteurs et services aussi divers que les réseaux sociaux, les navigateurs web, les réseaux de diffusion de contenu (*Content Delivery Network* - CDN), NFT*, les systèmes d'identité, l'internet des objets, la finance décentralisée, les places de marchés ou encore dans le domaine des données et de l'apprentissage machine.

Par exemple **Filecoin**, développé par Protocol Labs à l'origine d'IPFS est un service de cloud décentralisé. IPFS peut être utilisé par des sites web sans rapport avec les blockchains, comme Wikipedia, qui a développé un miroir de leur site web afin de donner accès à l'encyclopédie en ligne dans les pays où il est censuré. Ou encore **Audius**, un système décentralisé de streaming musical dont le contenu est hébergé sur IPFS.

Hébergement décentralisé de dApps* et de nœuds blockchain

La plupart des nœuds des blockchains publiques présentent aujourd'hui un certain degré de centralisation architecturale ou /et politique (voir Introduction - Qu'est-ce qu'une blockchain ?).

La centralisation architecturale revient à se poser la question de savoir de combien d'ordinateurs physiques est constitué le système. La centralisation politique consiste, quant à elle, à se demander combien d'individus ou d'organisations ont l'ultime contrôle des ordinateurs qui composent le système¹¹.

Or bon nombre de blockchains publiques hébergent certains nœuds de leur réseau sur des serveurs privés virtuels (*Virtual Private Server* - VPS), ce qui revient à centraliser à nouveau leur système puisque les ordinateurs physiques se retrouvent chez Amazon Web Service ou d'autres services de *Cloud* centralisés.

Pour remédier à cette contradiction, des *startups* proposent aux blockchains publiques une solution d'hébergement distribuée de leurs applications comme **Substratum**, **The Safe Network**¹² (voir Chapitre « Communications électroniques et télécommunications ») ou encore **DAppNode**, qui offre un service de déploiement et d'hébergement

10 « Ecosystem directory », IPFS, retrieved June 3, 2022, <https://ecosystem.ipfs.io/?results=70>

11 « The meaning of Decentralization », Vitalik Buterin, Medium, February 6, 2017, <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

12 « How Does it work ? », The Safe Network, retrieved June 3, 2022, <https://safenetwork.tech/>



d'applications décentralisées (DApps*), d'applications pair-à-pair ou encore de nœuds blockchain.

DAppNode¹³ est une plateforme gratuite et *open source* pour « déployer et héberger des DApps*, des clients P2P et des nœuds blockchain ». Pour l'utilisateur, DAppNode prend la forme d'une plateforme qui lui permet de déployer des applications décentralisées et des nœuds de blockchain sur leur propre machine et d'y accéder directement *via* un protocole décentralisé sans utiliser de passerelles ou de tiers centralisés.

DAppNode dispose d'un DAppStore où les applications disponibles peuvent être téléchargées et installées en quelques clics. DAppNode permet enfin à leurs utilisateurs de gagner des tokens en participant à la maintenance, à la validation ou au partage des ressources de certains réseaux décentralisés.

Cloud décentralisé

Le marché traditionnel des services *Cloud* est entièrement dominé par quelques géants américains et chinois, appelés hyperscalers. Fin 2019, une dizaine d'acteurs se partageaient 77 % du marché mondial. En 2020, Amazon Web Services (AWS) détenait 31 % du marché

des infrastructures de *Cloud*, suivi par Microsoft Azure (20 %), Google Cloud 6 %, Alibaba 5 %¹⁴. En Europe, au premier semestre 2020, 68 % des dépenses d'infrastructures *Cloud* des entreprises européennes sont captées par Amazon Web Services (53 %), Microsoft Azure (9 %) et Google (6 %) alors que le Français OVHcloud, leader européen du cloud privé, n'en détient que 4 %¹⁵. Face à cette offre d'infrastructures centralisées d'hébergement se développe une offre de *Cloud* dit décentralisé, portée par plusieurs acteurs comme **Skynet (Sia)**, **Storj** ou encore **Arweave**, même si leur portée reste à ce jour encore limitée.

Si l'on compare le stockage des centres de données centralisés et le stockage décentralisé de données, le premier s'appuie sur des infrastructures construites *ex nihilo* pour opérer le service alors que le *Cloud* décentralisé s'appuie sur des capacités de stockage et de bande passante déjà existantes et fournies à la périphérie du réseau par les particuliers ou entreprises qui opèrent le service.

L'investissement matériel nécessaire à la construction de centre de données disparaît lorsque le service d'hébergement décentralisé s'appuie sur les ressources déjà existantes sur le réseau, dont les capacités sont de

13 « What is DAppNode ? », DAppNode, retrieved June 3, 2022, <https://docs.dappnode.io/get-started/intro>

14 « Global cloud services spend exceeds US\$50 billion in Q4 2021 », Canalys, February 3, 2022, <https://www.canalys.com/newsroom/global-cloud-services-Q4-2021>

15 « Le Cloud européen : de grands enjeux pour l'Europe et cinq scénarios avec des impacts majeurs d'ici 2027-2030 », Jacques-André Fines Schlumberger, *La Revue Européenne des Médias et du Numérique* - N°57-58 Printemps - été 2021, <https://la-rem.eu/2021/10/le-cloud-europeen-de-grands-enjeux-pour-leurope-et-cinq-scenarios-avec-des-impacts-majeurs-dici-2027-2030/>

facto nettement supérieures. Si les entreprises ont entamé depuis plusieurs années la migration de leurs données vers des tiers spécialisés, le coût afférant à l'hébergement de ces données augmentent considérablement au fur et à mesure qu'elles s'accumulent.

Or « *la capacité inutilisée des capacités de stockage des particuliers est aujourd'hui tellement excédentaire que les coûts peuvent rester bas et n'ont pas besoin d'augmenter en fonction de la croissance des données*¹⁶ ». Plusieurs initiatives blockchain tirent partie de ces nouvelles architectures d'hébergement de données.

Skynet est construit au-dessus d'une blockchain publique appelée **Sia**, lancée en 2015. C'est un protocole ouvert pour l'hébergement de données et d'applications décentralisées. Les fondateurs du projet décrivent leur service comme un « *Airbnb pour le stockage de données*¹⁷ ». Des personnes qui ont besoin d'un espace de stockage (appelés Loueurs/*Renters*) paient, à l'aide d'un token* appelé **Siacoïn**, pour stocker leurs données sur les disques durs de personnes qui disposent d'un espace de stockage inutilisé (appelés Hôtes/*Hosts*). Le service opéré par Sia consiste à chiffrer les données, les découper en paquets, et les distribuer sur tous les ordinateurs qui participent au système.

Comme il n'y a pas d'autorité centrale, les contenus ne peuvent pas être censurés. Tout comme **Storj DCS**, pour Decentralized Cloud Storage, dont un premier livre blanc, paru en décembre 2014 a été mis à jour en 2016 et dont la plateforme a été lancée fin 2018¹⁸. Des personnes disposant d'espace de stockage inutilisé peuvent ainsi participer au réseau de *Cloud* décentralisé en devenant un nœud du réseau et seront payés en tokens Storj pour le service rendu. Pour citer un dernier projet, **Arweave** est un réseau de stockage décentralisé « *qui vise à proposer une plateforme pour le stockage de données permanent* » et se décrit comme « *un disque dur collectif qui n'oublie jamais*¹⁹ ». Présenté sous le nom de Archain en août 2017, renommé en Arweave en février 2018, le service est lancé en juin de la même année et héberge un certain nombre d'applications décentralisées et de plateformes communautaires.

Streaming vidéo décentralisé

Live Peer, créé à New York en 2017 et construit sur la blockchain publique Ethereum, est une plateforme décentralisée de diffusion de vidéo en direct. L'un des postes de dépense parmi les plus importants pour une plateforme de vidéo en *streaming* est le coût du transcodage des vidéos.

16 « Comparing the Economics of Centralized and Decentralized Cloud Storage », Christine Ackley, Storj, July 15, 2021, <https://www.storj.io/blog/comparing-the-economics-of-centralized-and-decentralized-cloud-storage>

17 « Skynet Overview », Siasky, retrieved May 30, 2022, <https://support.siasky.net/>

18 « Getting Starting on DCS », Storj, retrieved May 30, 2022, <https://docs.storj.io/>

19 « Arweave », Arweave.org, retrieved May 30, 2022, <https://www.arweave.org/>



Le transcodage d'une vidéo est le processus qui consiste à optimiser le fichier brut d'une vidéo pour le reformater selon différentes tailles afin d'en optimiser la lecture quelle que soit la bande passante et l'appareil de celui qui la visionne. Selon LivePeer, « *ce processus coûte environ 3 dollars par flux et par heure à un service Cloud comme celui d'Amazon, jusqu'à 4 500 dollars par mois pour un serveur de médias, et jusqu'à 1 500 dollars par mois pour un réseau de diffusion de contenu²⁰* » (*Content Delivery Network - CDN*).

La promesse de LivePeer réside en un protocole destiné aux développeurs informatique, permettant de proposer un service de vidéo en direct ou à la demande avec une réduction du coût par cinquante²¹.

Lorsqu'une personne enregistre ou filme en direct, à partir d'une application ayant intégré le service de Livepeer, le flux vidéo est envoyé sur le réseau pair-à-pair et transcodé par certains des nœuds du réseau appelés « orchestrateurs ». Les orchestrateurs exécutent un logiciel qui met à disposition les ressources de leur ordinateur (CPU, GPU et bande passante) afin de transcoder et distribuer la vidéo sur le réseau Livepeer. Pour cette activité, ils sont rémunérés en Ether ou en crypto-actif stable* comme le DAI.

Pour opérer sur le réseau, les orchestrateurs acquièrent auparavant un token appelé Livepeer token (LPT). Plus un orchestrateur dispose de token LPT, plus il est en mesure d'effectuer de travail de transcodage sur le réseau et être rémunéré. Un seconde type d'utilisateur, appelé « délégué », sont des détenteurs de tokens LPT qui participent à la sécurité du réseau en plaçant leurs tokens auprès des orchestrateurs de leurs choix.

Ainsi, lorsqu'un média utilise le service de *streaming* vidéo de Livepeer, il paye au réseau des frais, bien moins élevés que sur une plateforme centralisée, qui seront reversés aux orchestrateurs et aux délégués. Le protocole Livepeer crée également de nouveaux tokens LPT et les répartit entre les orchestrateurs et les délégués en fonction de leur participation par rapport aux autres membres du réseau, ce qui permet « *d'accroître la propriété du réseau auprès de ceux qui participent et de la réduire parmi ceux qui ne participent pas²²* ».

Ces nouveaux tokens sont créés selon un taux d'inflation qui s'ajuste automatiquement en fonction du nombre de tokens mis en jeu par rapport à l'offre totale en circulation, afin notamment de « *trouver un compromis sain entre la sécurité du réseau et la liquidité des tokens²³* ». Selon Livepeer, 4 250 délégués sécurisent à ce jour le réseau.

20 « Livepeer », Livepeer, retrieved May 30, 2022, <https://livepeer.org/primer>

21 *Ibid.*

22 *Ibid.*

23 *Ibid.*

Si tous ces services proposent de repenser la manière dont les contenus, les données et les applications sont hébergés, une entreprise américaine, **Mediachain**, créée en 2016 et rachetée par Spotify en 2017, construit un index décentralisé de données (voir *infra*). Un index est la structure de données utilisée par un système de gestion de base de données pour retrouver rapidement les données en son sein.

Média et journalisme

Les médias d'information et le journalisme, notamment depuis l'avènement des réseaux sociaux, s'adaptent à la perte de leur monopole sur la parole publique depuis les années 2010 et l'avènement du web participatif.

Les défis auxquels les médias d'information sont confrontés sont nombreux : la lutte contre les fausses informations et la crise de confiance dont certains font l'objet, la monétisation de leurs contenus, les difficiles rapports avec les géants du web (puissants vecteurs d'audience, que ce soit de la part de Google pour la recherche d'information, mais aussi de la part des réseaux sociaux, notamment de Meta ex Facebook), la pression publicitaire portée notamment par la publicité programmatique, dont le modèle repose sur un profilage toujours plus poussé de leur audience.

Il y a sept ans, plusieurs projets blockchain portés par des journalistes, et abandonnés depuis, ont ainsi vu le jour, parmi lesquels **Civil.co**, créé en 2016 et dont l'activité a cessé en 2020, ou encore **Po.et**, créé la même année et arrêté en 2019. Le projet Civil.co était de créer un token offrant la possibilité aux journalistes d'être rémunérés directement par leurs lecteurs, sans passer par un média. Selon son président à l'époque, Matthew Iles, l'idée était de « tirer parti des blockchains et de la crypto-économie et créer une plateforme de presse libre et indépendante n'impliquant que des journalistes et des citoyens, sans aucune publicité ni aucun tiers dans le modèle économique²⁴ ».

Le projet *open source* Po.et, quant à lui, se présentait comme « un protocole décentralisé pour la propriété du contenu, leur découverte et leur monétisation dans les médias ». Po.et s'adressait aux créateurs de contenus (journalistes, médias, YouTubers, podcasters, blogueurs, artistes...) pour certifier et protéger leurs œuvres, en les horodatant dans la blockchain Bitcoin et en y associant des métadonnées (nom de l'auteur ou du premier éditeur), ainsi que les licences d'exploitation. Ces informations étaient stockées *via* le logiciel libre InterPlanetary File System (IFPS) (voir *supra*). Il devient alors possible de tracer l'utilisation d'un contenu et de vérifier si le droit d'auteur a été respecté.

24 « Quelles synergies entre les blockchains et les industries culturelles ? », Jacques-André Fines Schlumberger, *La Revue Européenne des Médias et du Numérique* - N°49 Hiver 2018-2019, <https://la-rem.eu/2019/03/quelles-synergies-entre-les-blockchains-et-les-industries-culturelles/>



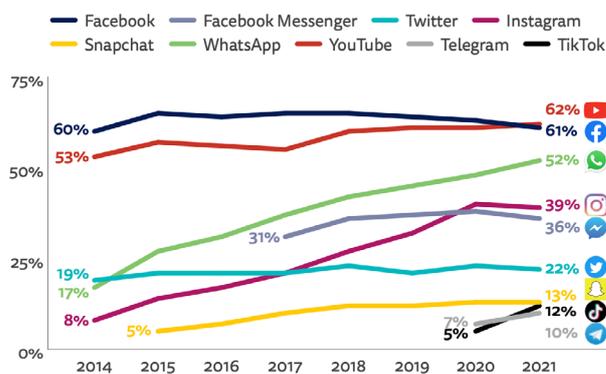
Dans le domaine cette fois, de la lutte contre les fausses informations, une entreprise française, **Block Expert**, tout comme **MadNetwork** créé à New York en 2017, avaient lancé un label, nommé **Safe.press** pour le premier et **Full Transparency** pour le second. Ils permettaient de certifier les communiqués de presse des entreprises, dont le détournement de la communication peut causer d'importants préjudices.

Pour ne citer qu'un seul exemple, le 22 novembre 2016, un communiqué du groupe Vinci annonçait une révision des comptes financiers, ainsi que le renvoi de son directeur financier, faisant rapidement plonger le cours de l'action de 19 %, soit l'équivalent de 6 milliards d'euros. Or le communiqué était faux. Le label Safe.press construit sur une blockchain privée en 2019, développée sur Hyperledger, a cessé ses activités début 2020, tout comme **MadNetwork**.

Force est de constater que le caractère décentralisé des blockchains n'a pas trouvé d'écho au sein des médias d'information traditionnels. Quelques innovations ont cependant émergé dans le domaine des réseaux sociaux et des micro-paiements.

Réseaux & Médias sociaux

PROPORTION THAT USED EACH SOCIAL NETWORK FOR ANY PURPOSE IN THE LAST WEEK (2014-21) - AVERAGE OF 12 MARKETS



Q12a. Which, if any, of the following have you used in the last week for any purpose? Base: Total 2014-21 sample in selected markets (most n = 2000). Note: From 2015-21 the 12 countries included are UK, USA, Germany, France, Spain, Italy, Ireland, Denmark, Finland, Japan, Australia and Brazil. In 2014, we did not poll in Australia or Ireland.

Source : Reuters Institute Digital News Report 2021 10TH Edition Nic Newman with Richard Fletcher, Anne Schulz, Simge Andi, Craig T. Robertson, and Rasmus Kleis Nielsen https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf

En janvier 2022, 4,62 milliards de personnes dans le monde utilisent un ou plusieurs réseaux sociaux²⁵, soit 58,4 % de la population mondiale. Les réseaux sociaux les plus populaires sont détenus par Meta (Facebook), Google, Twitter et Snap Inc. Leur formidable audience et leur succès commercial coïncident avec toute une série de critiques portant notamment sur la manipulation des contenus, les fausses informations, le détournement de publicités à des fins politiques, la censure, opérée directement par le réseau social, ou par un pays qui décide de suspendre ou d'en couper définitivement l'accès à

25 « Digital 2022: une nouvelle année de croissance exceptionnelle », We Are Social, retrieved June 3, 2022, <https://wearesocial.com/fr/blog/2022/01/digital-2022-une-nouvelle-annee-de-croissance-exceptionnelle/>

ses ressortissants, le modèle d'affaire, et des critiques basées sur la captation et l'analyse de données personnelles à l'insu de leurs utilisateurs.

Des projets blockchains s'attèlent à proposer de nouveaux modèles adressant quelques-unes de ces problématiques, notamment en créant un réseau social décentralisé, comme **Steem**, **Hive** ou **Dtube**, mais également des solutions de micropaiement comme **Kin**.

Dans son livre blanc publié en août 2017²⁶, Steem se présente comme « *une plateforme incitative de contenu public basée sur une blockchain* ». Steem est une blockchain publique au-dessus de laquelle sont construites des applications décentralisées (dApps*) dont la première, **Steemit**, souvent comparée au réseau social Reddit.com, a été lancée le 4 juillet 2016. Steemit se présente « *comme la première base de données accessible au public pour du contenu stocké de manière immuable sous forme de texte brut, avec un mécanisme d'incitation intégré*²⁷ ». La blockchain est publique et *open source*²⁸. Le mécanisme de consensus mis en oeuvre est la preuve d'enjeu déléguée (Delegated Proof of Stake - DPoS*).

Steemit rémunère à la fois les créateurs de contenu sur la plateforme, ainsi que les personnes qui votent et aiment

les contenus afin d'identifier ceux de qualité à travers un système combinant une « réserve de récompense » (*pool rewarding*) couplé à un « système de vote »²⁹.

Les tokens de STEEM sont générés à un rythme fixe d'un bloc toutes les trois secondes. Plus précisément, la blockchain Steem génère des tokens STEEM à un taux fixé à 9,5 % par an depuis décembre 2016, avec un taux d'inflation qui diminue de 0,5 % par an avant de cesser lorsqu'il atteindra 0,95 % dans 20,5 ans. L'ensemble des tokens STEEM générés sont alloués ainsi : 75 % sont envoyés dans la réserve de récompense, et sont distribués aux créateurs de contenus et à ceux qui votent pour ces contenus. 15 % des tokens sont distribués à ceux qui possèdent déjà un certain type de token, appelé Steem Power (voir *infra*), et les 10 % restants sont distribués à des nœuds sur la blockchain Steem, appelés délégués, élus pour valider les blocs de transaction sur la blockchain.

Steemit s'appuie sur trois tokens gérés *via* la blockchain publique Steem : le Smart Media Token (SMT) appelé (1) STEEM, le token natif de la blockchain du même nom, le (2) Steem Power (SP), une version verrouillée de STEEM qui donne au compte une influence sur la plateforme et le (3) Steem Backed Dollar (SBD) dont la valeur correspond à

26 « Steem White Paper », Steem, August 2017, <https://steem.com/SteemWhitePaper.pdf>

27 « Steem Developer Portal », Steem, retrieved June 3, 2022, <https://developers.steem.io>

28 « Steem/Steemit », Github, retrieved June 3, 2022, <https://github.com/steemit/steem>

29 « A protocol for enabling smart, social currency for publishers and content businesses across the internet », Steem, Bluepaper, retrieved May 31, 2022, <https://steem.com/steem-bluepaper.pdf>



un dollar en STEEM. Lorsqu'un rédacteur reçoit une récompense pour le contenu qu'il a publié, ou un curateur pour le vote qu'il a effectué, la moitié de la récompense est versée sous la forme de Steem Power (SP), et l'autre moitié sous la forme de Steem Backed Dollar (SBD), avec la possibilité de convertir mutuellement les tokens entre eux ou en STEEM.

Mais lorsqu'un utilisateur vote sur un contenu, son influence sur la distribution du pool de récompenses est directement proportionnelle à la quantité de Steem Power (SP) qu'il détient. Pour avoir une influence sur le réseau, les utilisateurs les plus actifs qui conservent leur Steem Power, sont ainsi récompensés.

L'innovation apportée par Steemit est d'avoir créé un réseau social qui permet aux éditeurs de contenus de ne pas reposer sur un modèle publicitaire, de prendre en charge nativement des micro transactions dont le règlement est quasi instantané et les frais de transaction quasi nuls, et d'opérer un cercle vertueux entre ceux qui publient et ceux qui votent, les deux étant récompensés pour leurs activités.

En mars 2020, Steemit a été racheté par la fondation Tron, dirigée par Justin Sun, ce qui a provoqué le mécontentement d'une partie de la communauté Steem

et s'est soldé par un *hard fork** de la blockchain, donnant naissance à **Hive**. Selon leurs concepteurs, **Hive** est « *une blockchain avec une gouvernance de type DPOS [Delegated Proof of Stake], construite à partir d'une copie du code source de Steem et qui fonctionne de manière totalement indépendante de la chaîne existante*³⁰ ».

Que ce soit sur les blockchains publiques comme STEEM ou Hive, des porteurs de projets peuvent construire des applications décentralisées (dApps*), parmi lesquelles **D.tube**, une plateforme décentralisée de vidéo ou encore **Peakd**³¹ ou **Ecency**³², des réseaux sociaux décentralisés.

La plateforme **DTube** propose ainsi un réseau de partage de vidéos où certains utilisateurs postent des vidéos alors que d'autres déterminent l'intérêt des contenus. Non seulement les utilisateurs peuvent donner des « pourboires » aux créateurs de contenu, mais aussi leurs « j'aime » et leurs commentaires, qui seront rémunérés par la plateforme, comme sur Steemit.

La plateforme autonome, est contrôlée par dix personnes ou leaders³³, choisis par la communauté, et qui seront en charge de produire les nouveaux blocs de transactions. La plateforme se décrit comme étant résistante à la censure, affranchie du modèle de la publicité,

30 « Announcing the Launch of Hive Blockchain », hiveio, March 17, 2020, retrieved May 31 2022, <https://peakd.com/communityfork/@hiveio/announcing-the-launch-of-hive-blockchain>

31 « Decentralized Social Media with True ownership », Peakd, retrieved July 21, 2022, <https://peakd.com/>

32 « Welcome to Ecency », Ecency, retrieved July 21, 2022, <https://ecency.com/>

33 Ce chiffre peut varier dans le futur.

et affirme de ne pas collecter des données utilisateurs tout en distribuant 90 % de la valeur créée³⁴.

Ces plateformes décentralisées de contenus, s'appuyant sur des blockchains publiques pensées pour favoriser des micro-transactions autour de contenus gérés par une communauté d'utilisateurs, restructurent les dynamiques à l'œuvre entre ses utilisateurs et proposent de nouveaux paradigmes de compensation et de récompense quant à la participation de chacun³⁵.

L'un des points fondamentaux de ces applications est leur capacité à monétiser les interactions de leurs utilisateurs, non pas à leur insu comme c'est le cas avec les réseaux sociaux classiques, mais à l'aide de tokens, échangés directement par les utilisateurs au sein de communautés.

Arts, Musique & Vidéo

L'Objectif de développement durable 11, « *faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables* » a pour ambition, à travers sa cible 4 le « *renforcement des efforts de protection et de préservation du patrimoine culturel et naturel mondial*³⁶ ».

Les industries de l'art, de la musique, des films et de la culture en général ont profondément été impactées par le développement du web.

Après les promesses d'une désintermédiation entre les artistes et leur public dans les années 2000, force est de constater qu'aujourd'hui, la valeur est toujours plus captée par des intermédiaires de plus en plus puissants. Pour ne citer qu'un exemple, si l'industrie musicale génère 43 milliards de revenus annuels par an, seuls 12 % reviennent aux artistes³⁷.

L'une des raisons de ce déséquilibre provient du nombre d'intermédiaires entre les artistes et leur audience, ainsi que de la manière dont la valeur circule entre eux.

34 « A new model: the social blockchain », D-Tube, retrieved July 21, 2022, <https://token.d.tube/>

35 « How The Blockchain Can Solve Social Media's Biggest Problems » Sunny Dhillon, Forbes, February 28, 2018, <https://www.forbes.com/sites/valleyvoices/2018/02/28/how-the-blockchain-can-solve-social-medias-biggest-problems>

36 Objectif de développement durable 11, Nations Unies : Faire en sorte que les villes et les établissements humains soient ouverts à tous, sûrs, résilients et durables, <https://www.un.org/sustainabledevelopment/fr/cities/>

37 « Introducing \$AUDIO, The Audius Platform Token », October 8, 2020, <https://medium.com/audius/introducing-audio-the-audius-platform-token-2c575215b439>. retrieved June 1, 2022.



Un certain nombre d'initiatives blockchain souhaitent bousculer ce paysage hyper centralisé en redonnant au créateur d'œuvres de l'esprit, l'opportunité de nouvelles sources de financement, une meilleure maîtrise des droits par l'artiste lui-même, la gestion et la programmabilité des droits associés et des micro transactions favorisant également l'accélération des délais de paiement.

Ces initiatives blockchain reposent tout à la fois sur le développement des NFT*, poussés par l'engouement qu'ils suscitent depuis le début de l'année 2021, mais également sur la création de nouveaux écosystèmes reliant directement artistes et audience à travers le token de plateformes décentralisées.

Comme nous l'avons vu au chapitre « Aide, Charité et Philanthropie », les tokens non fongibles (*Non Fungible Token* - NFT*), associés au domaine de l'art et des contenus numériques, inaugurent de nouvelles formes de financement de projets à dimensions sociale et/ou environnementale, qu'ils soient portés par des organisations déjà existantes ou bien par des communautés de personnes réunis autour d'une cause.

Comment fonctionne un token non fongible* (*Non fungible token* - NFT) ?³⁸

Si bitcoin et la majorité des crypto-actifs émis grâce à une blockchain publique sont fongibles, c'est-à-dire que n'importe lequel de ces tokens peut être échangé contre un autre, les tokens non fongibles désignent quant à eux un actif numérique unique. Ils sont émis sur une blockchain publique comme Ethereum, Tezos ou encore Cosmos, à l'aide d'un *smart contract** et reposent par conséquent sur les qualités intrinsèques des blockchains publiques.

Cependant, outre leur caractère infalsifiable, traçable, interopérable et échangeable, un token non fongible est unique et indivisible. Cette unicité permet de certifier l'authenticité et la propriété d'objets originaux, parmi lesquels des œuvres d'art, des objets de collection, physiques ou numériques, ou encore des noms de domaines, des créances et même des biens immobiliers.

Pour exister, à l'instar d'une monnaie nationale frappée par un État, un NFT est d'abord « frappé » dans une blockchain publique, en anglais *minted*, puis par la suite éventuellement « brûlé », en anglais *burnt*, c'est-à-dire supprimé. *Minting an NFT*, « frapper un NFT », consiste, à partir d'un portefeuille* (*wallet*) et d'un *smart contract**, à enregistrer le token et ses données d'identification dans une

38 « NFT », Jacques-André Fines Schlumberger, *La revue européenne des médias et du numérique*, N°57-58 Printemps - été 2021, <https://la-rem.eu/2021/07/nft/>

blockchain publique afin qu'il devienne immuable, échangeable mais aussi consultable et vérifiable par quiconque.

Plusieurs blockchains publiques comme **Binance Smart Chain, Polygon, EOS, Flow, Polkadot, Tezos, Tron** ou encore **WAX** sont utilisées pour y frapper un NFT, la plus populaire étant la blockchain **Ethereum**.

Sur celle-ci, un NFT a fait l'objet d'un *smart contract** qui applique les spécifications ERC-721 ou ERC-1155. Chaque token non fongible est assorti d'un identifiant dans le *smart contract**. L'association « adresse du contrat » et « identifiant » devient alors un identifiant unique au monde, un *hash**. Seul le *hash**, et non l'œuvre, est stocké dans la blockchain Ethereum et sert à prouver la propriété du contenu aux yeux de tous. L'acquisition d'un NFT n'empêche pas l'œuvre numérique, l'image, l'animation, la carte à collectionner ou la vidéo d'être vue et partagée par d'autres. La norme prévoit également une fonction de transfert entre portefeuilles, afin de permettre les transactions de NFT tout en faisant apparaître l'ensemble des propriétaires au fur et à mesure des échanges.

En outre, des métadonnées associées au NFT fournissent des informations descriptives. Lorsqu'un NFT correspond à un billet de concert, les métadonnées pourront désigner par exemple la date de l'évènement et le type de billet, en plus du nom du concert, de ses coordonnées et de son programme.

L'œuvre en elle-même, dès lors qu'elle est numérique, est accessible sur le web, ce qui induit un risque de disparition du contenu. Elle peut également être hébergée via des systèmes de stockage décentralisés, tel que IPFS (voir *supra*) pour en garantir un accès pérenne.

Tout d'abord, les blockchains peuvent être utilisées comme des registres distribués permettant d'enregistrer la paternité d'une œuvre et tout fichier numérique se prête naturellement à l'enregistrement de son empreinte dans une blockchain publique. De nombreuses entreprises proposent ce type de service depuis plusieurs années comme **Binded** aux Etats-Unis depuis 2016, **BlockchainyourIP** en France depuis 2017 ou encore **HashingDNA** en Espagne depuis 2018. Le procédé consiste à créer un certificat comprenant une empreinte numérique du document, sous la forme d'un *hash** (fonction mathématique qui transforme n'importe quel contenu sous la forme d'un nombre hexadécimal et qui, à la moindre modification du contenu, donnera un nombre totalement différent), la date de son enregistrement dans la blockchain utilisée ainsi que le numéro de la transaction et celui du bloc où l'empreinte numérique du document a été enregistrée.

Au-delà de la preuve de paternité d'une œuvre, les blockchains, et tout particulièrement les *smart contracts** permettent d'imaginer de nouveaux systèmes de gestion des droits d'auteur, régulièrement dénoncés par les artistes

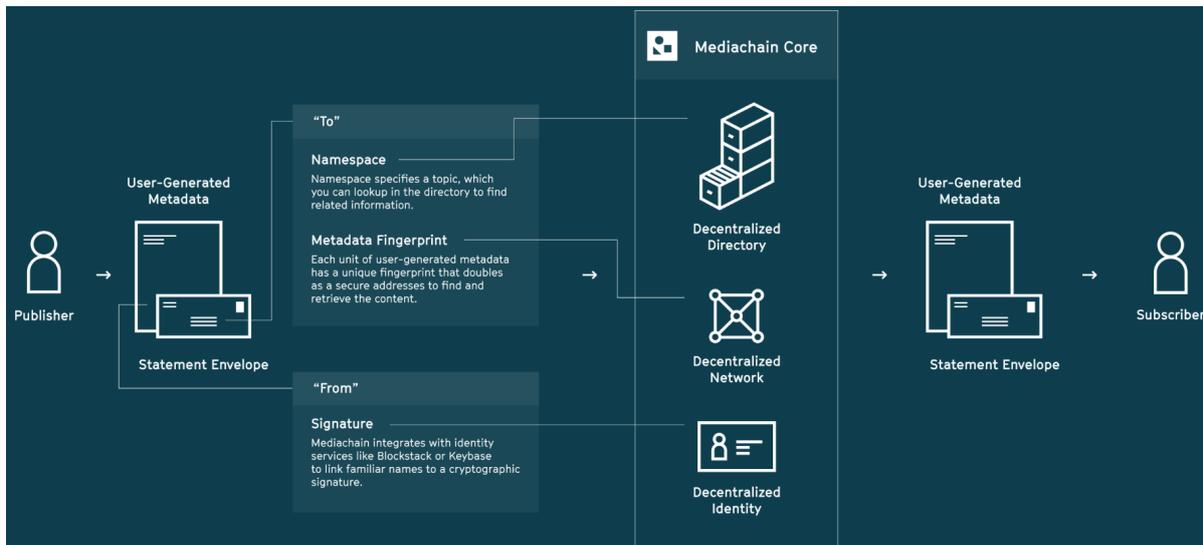


Schéma de l'utilisation de Mediachain

Source : « Mediachain », retrieved June 1, 2022, <http://www.mediachain.io/>

dont les règlements opérés par des sociétés de gestion collective peuvent prendre des mois, voire des années, ou même ne jamais arriver aux bénéficiaires.

La plupart des artistes dénoncent également la faiblesse des montants perçus pour une écoute sur les plateformes de *streaming*, qu'elles soient audiovisuelles ou musicales. Selon le site Digital Music News, la somme moyenne versée par YouTube aux artistes pour chaque écoute est passée de 0,0006 \$ en 2017 à 0,00074 \$ en 2019 et la somme moyenne versée par Spotify est de 0,004 \$³⁹.

Les blockchains, semble-t-il, apporteraient non seulement de la transparence à une chaîne de valeur particulièrement opaque, en court-circuitant certains intermédiaires, mais simplifieraient considérablement le paiement des artistes tout en s'adaptant aux nouveaux usages, notamment ceux qui sont liés à l'écoute de musique en *streaming*.

Mediachain⁴⁰, créé à New-York en 2016, est un index décentralisé de données. Mediachain se définit ainsi comme « *un espace logique unique, organisé par thème ou par application, permettant à de multiples participants de publier et de découvrir des données sans point central de contrôle ou de défaillance.*

39 « How Much Does Spotify Pay Per Stream ? Here's the Latest Data (Updated for 2022) », Dylan Smith, digitalmusicnews.com, August 17, 2020, <https://www.digitalmusicnews.com/2020/08/17/how-much-does-spotify-pay-per-stream-latest/>

40 « Mediachain », Mediachain, retrieved June 21, 2022, <http://www.mediachain.io/>

En d'autres termes, Mediachain permet à de multiples participants de collaborer à des index de données de manière totalement décentralisée⁴¹ ».

L'un des problèmes auquel MediaChain tente d'apporter une réponse est celui de l'opacité de l'attribution des droits d'auteurs, notamment dans le domaine de la musique. L'idée de créer un index décentralisé, commun, ouvert et distribué, regroupe les informations relatives aux droits d'auteurs, jusqu'alors éparpillées dans les différents labels musicaux. Le registre ouvert de MediaChain utilise les métadonnées liées aux œuvres (nom de l'artiste, type de contrats, droits d'auteurs, ...) pour les référencer dans un index accessible à tous les professionnels. Ces métadonnées sont ensuite hachées et stockées dans IPFS (voir *supra*). MediaChain permettrait ensuite d'accéder à une cartographie des métadonnées liées aux œuvres stockées dans IPFS. En 2017, Mediachain a été racheté par Spotify, régulièrement condamné pour des infractions aux droits d'auteur, sans qu'il ne soit toutefois possible de connaître l'avancement du projet à ce jour.

Ces plateformes centralisées de *streaming* musical voient également l'émergence de nouveaux acteurs sur leur marché. **Audius**⁴², créé en 2017, est une plateforme de *streaming* musical en pair-à-pair, mettant en relation directement les artistes avec leur audience, auprès de laquelle une application iOS ou Android est disponible depuis 2020. D'abord construite sur Ethereum, Audius a migré sur la blockchain publique Solana⁴³ en 2021.

Audius fonctionne comme une plateforme de *streaming* classique : les artistes sont rémunérés en fonction du nombre d'écoutes générées sur la plateforme et perçoivent un pourcentage de rétribution bien plus élevé que sur des plateformes classiques comme Spotify ou Deezer. Selon la plateforme, 90 % des revenus générés sur Audius sont reversés aux artistes⁴⁴. Les artistes, rémunérés avec le token natif de Audius, le \$AUDIO, pourraient prochainement créer leur propre token, indexé sur le \$AUDIO.

La gouvernance de la plateforme est directement assurée par des membres de la communauté qui mettent en jeu (*proof of stake**) une somme d'argent en \$AUDIO et dont les droits de vote

41 « Mediachain an open, universal media library », Mediachain, retrieved June 21, 2022, <http://docs.mediachain.io>

42 « Audius », Audius, retrieved June 1, 2022, <https://audius.co/>

43 « L'industrie musicale, future victime de la Révolution blockchain ? Audius (Audio) au sommet des charts ! », Hellmouth Banner, Le Journal du Coin, 26 Octobre 2021, <https://journalducoin.com/actualites/audius-donne-le-tempo-dune-industrie-musicale-blockchainisee/>

44 « Audius, la plateforme qui rémunère le mieux les artistes (et les auditeurs) ? », Cloé Gruhier, Hauméa Magazine, retrieved June 1, 2022, <https://www.haumeamagazine.com/audius-la-plateforme-de-streaming-qui-remunere-le-mieux-les-artistes-et-les-auditeurs/#:~:text=Audius%20est%20une%20plateforme%20de,%C3%A0%20la%20crypto%2Dmonnaie>



dépendent de la somme investie. Au sein du réseau Audius, les *discovery node* sont des noeuds chargés d'enregistrer les nouveaux artistes sur la plateforme, afin d'encourager l'ajout de nouveaux créateurs de contenus directement par la communauté⁴⁵ et les *content node* sont des noeuds chargés de valider la mise en ligne des contenus musicaux sur la plateforme⁴⁶. Tous deux perçoivent des \$AUDIO pour leur participation au réseau.

Pour inciter les membres de la communauté à sécuriser la plateforme en immobilisant leur tokens (*proof of stake**), plus l'utilisateur épargne ses \$AUDIO, plus il débloquent des fonctionnalités sur la plateforme, comme l'accès à des collections de NFT* ou encore l'accès privilégié à certains contenus. Audius, qui revendique plus de 6,2 millions d'utilisateurs actifs en mai 2022 est encore loin de ses concurrents comme Spotify ou Deezer, mais force est de constater que le projet prend de plus en plus d'ampleur.

Que ce soit dans le domaine de la musique ou même du cinéma, certaines initiatives blockchain visent à expérimenter de nouvelles sources de financement en impliquant notamment le grand public.

Inflow music, qui utilise Livepeer (voir *supra*), propose à des artistes, sportifs et

personnalités de créer leur propre token afin d'être directement financés par leurs fans qui, en échange, ont accès à des contenus exclusifs, des rencontres et des événements spéciaux accessibles uniquement aux détenteurs de tokens. Certains contenus, vendus sous la forme de NFT* pourront par la suite être revendus à d'autres acquéreurs, incluant, à chaque transaction, une commission de 15 % reversée à l'artiste. Inflow music se veut un moyen pour les artistes d'interagir sans intermédiaire avec leurs fans tout en bénéficiant de nouvelles sources de revenus. Inflow music, dont le service est encore en développement, a été incubé par l'accélérateur de *startups* du Web 3.0 Tachyon Accelerator, soutenu par ConsenSys et Protocol Labs⁴⁷.

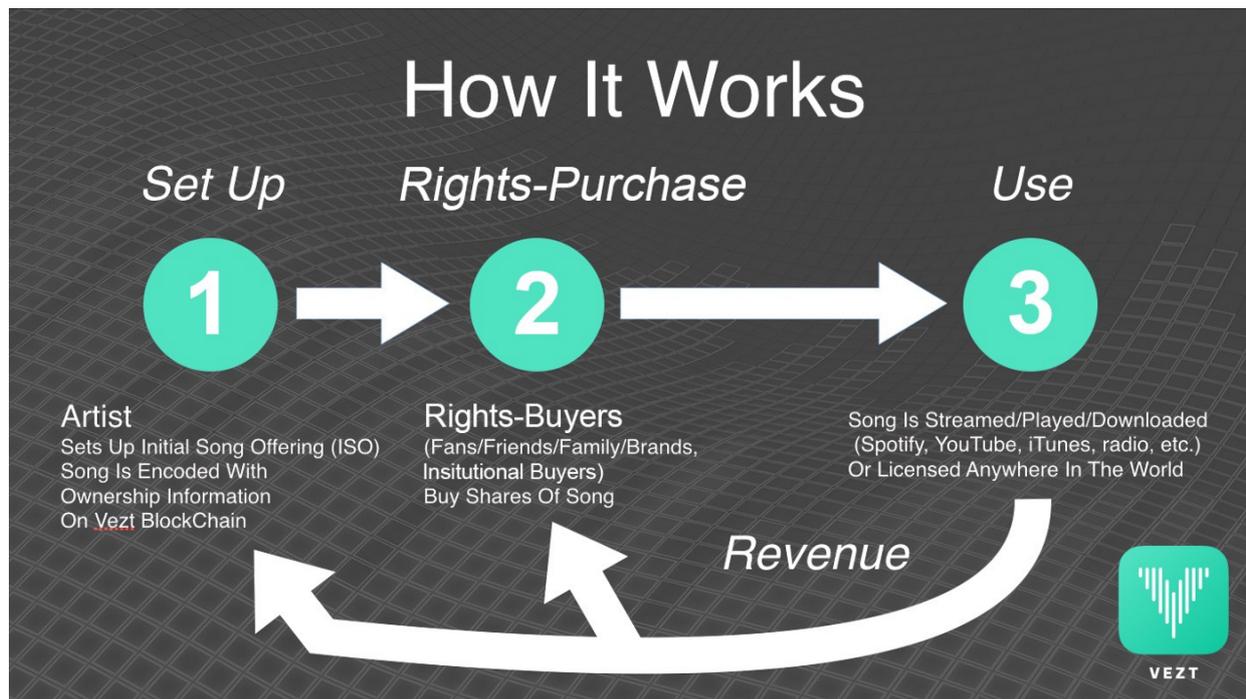
Vezt ou **Royal** proposent à des artistes de vendre une partie des royalties de leurs chansons écoutées en *streaming* sur les grandes plateformes d'écoute comme Spotify, Deezer ou Apple Music. **Vezt**⁴⁸, créée à Los Angeles aux États-Unis en 2017, est une application mobile de *streaming* musical construite sur la blockchain publique Ethereum, permettant à des artistes de mettre en vente une partie de leurs droits auprès de fans, qui seront ensuite rémunérés à hauteur de leur investissement initial. Plus précisément, Vezt met en vente certains droits d'auteur

45 « Audius, la plateforme qui rémunère le mieux les artistes (et les auditeurs) ? », Cloé Gruhier, Hauméa Magazine, consulté le 2 juin 2022, <https://www.haumeamagazine.com/audius-la-plateforme-de-streaming-qui-remunere-le-mieux-les-artistes-et-les-auditeurs/#:~:text=Audius%20est%20une%20plateforme%20de.%C3%A0%20la%20crypto%2Dmonnaie>

46 *Ibid.*

47 « How Inflow Created the First Music Platform for the Web3 Economy », Ivan Kreimer, Livepeer Video Services, May 26, 2022, <https://livepeer.com/blog/how-inflow-created-first-music-platform-web3-economy>

48 « Vezt », Vezt, retrieved June 1, 2022, <https://vezt.co>



How Vezt Works ?

Source : Vezt Inc, September 18, 2017, <https://medium.com/@vezt/the-real-greatest-hit-how-vezt-works-cb66aef74d67>

lors d'une campagne de financement participatif qu'ils appellent « *Initial Song Offering™ (ISO)*⁴⁹ » puis enregistre les droits de l'artiste auprès des sociétés de collecte de droits et des plateformes numériques, et les reverse ensuite au fur et à mesure, par le biais de *smart contracts**, aux artistes et aux acheteurs des droits selon le schéma en page d'après.

Par exemple, un artiste choisit une chanson et la date à laquelle vont être vendus les droits, par exemple 1000 \$ pour 1 % de leurs droits d'auteur, ainsi que la durée pendant laquelle les acheteurs vont être rémunérés, de trois ans, cinq ans, dix ans ou même à vie. Les acheteurs, notamment des fans, des professionnels

de la musique ou encore des marques achètent ces droits, dont l'artiste reçoit les fonds immédiatement. Les informations relatives aux droits de la chanson sont ensuite encodées sur la blockchain de Vezt et « *les redevances sont collectées à la fois auprès des sociétés de collecte de droits dans 137 pays du monde et auprès de STEM.is*⁵⁰, un service qui regroupe les redevances de performance numérique des services de streaming tels que Spotify, iTunes, YouTube, Pandora, etc.⁵¹ »

Royal fait la même chose. C'est une plateforme qui vend les droits de chansons créées par des artistes sous la forme de NFT*.

49 « The Real Greatest Hit: How Vezt Works », Vezt Inc, Medium, September 18, 2017, <https://medium.com/@vezt/the-real-greatest-hit-how-vezt-works-cb66aef74d67>

50 « Stem brings clarity to your modern music business », Stem, retrieved July 11, 2022, <https://stem.is/>

51 « The Real Greatest Hit: How Vezt Works », Vezt Inc, Medium, September 18, 2017, <https://medium.com/@vezt/the-real-greatest-hit-how-vezt-works-cb66aef74d67>



Les artistes choisissent le pourcentage des redevances de la chanson qu'ils souhaitent mettre en vente et le public achète ces droits de redevances de musique en *streaming* sous la forme de NFT*. Au fur et à mesure qu'une chanson est diffusée sur les différentes plateformes de *streaming* - Spotify, Apple Music, Youtube, etc., elle génère des redevances qui reviennent aux investisseurs initiaux selon les conditions définies dans les NFT*. Pour être accessible, le grand public peut procéder à l'achat de NFT* en utilisant le crypto-actif stable* USDC sur Polygon (Matic), et un portefeuille* comme Metamask, ou payer en carte de paiement traditionnel, la plateforme se chargeant de créer un portefeuille pour l'utilisateur.

L'artiste pourra également prévoir un certain nombre d'avantages liés au token. Le NFT* peut ensuite être revendu à un nouvel acheteur qui bénéficiera des redevances et avantages associés au token. Le projet est construit sur Polygon, un layer 2 basé sur la blockchain publique Ethereum. Créé en au début de l'année 2021, Royal comptait 120 000 inscrits en août. En deux tours de table opérés la même année, Royal a levé 71 millions de dollars, dont certains de la part d'artistes⁵². Ces deux initiatives, Vetz ou Royal,

semblent donc s'inscrire dans la continuité du système mis en place par les organismes traditionnels de collecte de droits d'auteurs et ne renouvellent que l'accès des droits d'auteur non plus aux seuls professionnels de la musique mais à leurs fans et aux particuliers.

Il est également possible d'imaginer, grâce aux *smart contracts**, d'assurer la multi-propriété de droits d'auteurs. La communauté Ethereum développe depuis le 15 septembre 2020 l'EIP-2981⁵³, un « NFT Royalty Standard » pour permettre aux *smart contracts** NFT⁵⁴ d'indiquer les redevances correspondant au créateur et aux propriétaires de droits d'auteur. La norme « *permet aux contrats, tels que les NFTs qui supportent les interfaces ERC-721 et ERC-1155, de signaler un montant de redevance à payer au créateur du NFT ou au détenteur des droits chaque fois que le NFT est vendu ou revendu*⁵⁵ ». Si le paiement des redevances n'est pas encore automatisé et reste manuel, le standard signale que, dans un futur EIP⁵⁶, un mécanisme serait proposé pour résoudre le paiement automatique et les notifications.

52 « Combining Music Rights with NFTs: Royal Raises Big Money », Carpenter Wellington PLLC, Lexology, December 9, 2021, <https://www.lexology.com/library/detail.aspx?g=92d81306-ca86-47ca-b570-34ad16483039>

53 « EIP-2981: NFT Royalty Standard », Zach Burks, James Morgan, Blaine Malone, James Seibel, Ethereum Improvement Proposals, September 15, 2020, <https://eips.ethereum.org/EIPS/eip-2981>

54 Par exemple ERC-721 et ERC-1155 sur la blockchain Ethereum.

55 « EIP-2981: NFT Royalty Standard », Zach Burks, James Morgan, Blaine Malone, James Seibel, Ethereum Improvement Proposals, Sep 15 2020, <https://eips.ethereum.org/EIPS/eip-2981>

56 Ethereum Improvement Proposals (EIPs) : proposition de normes spécifiant de nouvelles fonctionnalités sur Ethereum.

La *startup* Stendhal⁵⁷ a ainsi développé **Collab Splitter**⁵⁸, une application web qui permet aux artistes de créer et déployer un *smart contract** compatible avec ce standard Ethereum, afin de recevoir et répartir des paiements en crypto-actif selon des règles personnalisées.

Science décentralisée

Selon l'Institut de recherche pour le développement⁵⁹ (IRD), établissement public français placé sous la double tutelle des ministères de l'Enseignement supérieur, de la Recherche et de l'Innovation et de l'Europe et des Affaires étrangères, le lien entre le monde de la recherche et les Objectifs de développement durable a vocation est amené à se renforcer : « *si la place de certains acteurs pour atteindre les Objectifs de développement durables (États, ONG, organisations internationales...) peut faire évidence, ce n'est pas le cas de la recherche dont le rôle est méconnu dans ce domaine. Or la recherche est – ou va être – amenée à jouer un rôle de premier plan dans l'atteinte de ces objectifs à l'horizon 2030 : produire des connaissances et des données fiables, proposer des solutions innovantes, évaluer les progrès enregistrés. La recherche scientifique et l'innovation ont en particulier un rôle majeur à jouer dans les pays en développement, particulièrement*

*vulnérables et confrontés à de multiples défis, à la fois locaux et globaux (impacts du changement climatique, crises financières, pandémies, etc.)*⁶⁰ ».

Le monde de la recherche scientifique fait ainsi l'objet d'expérimentation de projets blockchain. Même si la plupart de ces initiatives sont peu matures, un mouvement, celui de la Science Décentralisée (*Decentralized Science*), semble émerger pour notamment, selon, Sarah Hamburg, neuroscientifique et porteuse du projet Lynx « *changer la façon dont la recherche est financée et les connaissances partagées et (...) transférer la propriété et la valeur loin des intermédiaires de l'industrie*⁶¹ ».

La Science décentralisée vise à expérimenter de nouvelles sources de financement, l'examen de recherche scientifique par les pairs, l'accès ouvert à des publications et des données scientifiques tout en garantissant l'anonymat des personnes dont les données personnelles sont utilisées.

Comme nous l'avons vu dans le chapitre Santé, un certain nombre d'applications autonomes décentralisées (DAO*) existent, comme **Molecule**, une plateforme qui permet à des scientifiques de partager leurs recherches et de présenter leurs projets

57 « Who we are ? », Stendhal, retrieved June 3, 2022, <https://stendhal.ai/>

58 « Split revenues from sales and royalties in a cheap, efficient and transparent way », Collab Splitter, retrieved June 21, 2022, <https://collab-splitter.org/>

59 « Une science engagée », IRD, retrieved July 21, 2022, <https://www.ird.fr>

60 « La recherche au service du développement, 17 objectifs pour un futur durable », 15 septembre 2020, <https://www.ird.fr/la-recherche-au-service-du-developpement-17-objectifs-pour-un-futur-durable>

61 « A Guide to DeSci, the Latest Web3 Movement », Sarah Hamburg, future.com, February 9, 2022, <https://future.com/what-is-decentralized-science-aka-desci/>



de façon structurée afin de se connecter à des collaborateurs et financeurs intéressés par leurs découvertes.

Ou encore **VitaDAO**, qui se présente comme une DAO* « *pour le développement de médicaments gouvernée par une communauté décentralisée et dont la principale mission est l'accélération de la recherche et du développement (R&D) dans le domaine de la lutte contre le vieillissement⁶²* », en s'appuyant sur des NFT* qui incorporent des contrats de licences de propriété intellectuelle.

Dans le domaine des évaluations scientifiques, **Ants Review** dénonce le fait que l'examen par les pairs et le contrôle de la qualité des publications scientifiques n'est ni rémunéré par les revues, ni apprécié à sa juste valeur par la communauté académique. Ants Review propose ainsi « *un système d'incitation basé sur la blockchain [Ethereum] qui récompense les scientifiques pour l'évaluation par les pairs des travaux d'autres scientifiques et qui renforce la confiance et la réputation⁶³* ».

Certains scientifiques voient également dans les NFTs* un moyen de lever des fonds pour financer leurs recherches. L'Université de Californie, Berkeley, a vendu aux enchères un NFT basé sur des documents du chercheur sur le cancer et Prix Nobel, James Allison pour 50 000 dollars⁶⁴.

Le créateur du *World Wide Web*, Tim Berners-Lee, a vendu aux enchères des fichiers horodatés contenant le code source de son invention sous la forme de NFT* et ainsi récolté 5,4 millions de dollars⁶⁵. Matt Stephenson, chercheur et fondateur de Planck Manuscripts⁶⁶ a vendu aux enchères un NFT représentant les résultats d'une étude empirique sur OpenSea⁶⁷, et compte utiliser les fonds pour répliquer l'étude avec plus de précision⁶⁸. Planck se décrit comme « *un système d'incitation visant à améliorer les incitations autour de l'innovation ouverte⁶⁹* ».

Dans le domaine de la santé, **Nebula Genomics** (voir Chapitre Santé), une entreprise de biotechnologie américaine créée en 2016, propose aux particuliers

62 « We're a DAO collective funding and advancing longevity research », VitaDAO, retrieved June 21, 2022, <https://www.vitadao.com/about>

63 « Ants-Review: A Privacy-Oriented Protocol for Incentivized Open Peer Reviews on Ethereum. », Bianca Trovò, Massari Nazzareno, January 22, 2021, *Euro-Par 2020: Parallel Processing Workshops*

64 « How scientists are embracing NFTs », Nicola Jones, Nature n°594, June 18, 2021, <https://www.nature.com/articles/d41586-021-01642-3>

65 « The World Wide Web's inventor sold its original code for \$5.4 million », Oscar Holland, CNN, retrieved June 21, 2022, <https://edition.cnn.com/style/article/tim-berners-lee-nft-auction>

66 « Non-Fungible Incentives for open innovation », Planck Manuscripts, retrieved June 21, 2022, <https://www.p1anck.com/>

67 « Open Source Science Manuscript 1 », Open Sea, <https://opensea.io/planck?tab=created>, retrieved June 21, 2022

68 « Launching the World's First Science NFT with Matt Stephenson from Planck », Unstoppable domains 62, Youtube, retrieved July 21, 2022, <https://www.youtube.com/watch?v=U4Rnso2Vpi0>

69 « Non-Fungible Incentives for open innovation », Planck Manuscripts, retrieved June 21, 2022, <https://www.p1anck.com/>

un séquençage de leur génome dont les données sont indéchiffrables et donne à leur client le contrôle de qui peut y accéder.

Il est alors possible de donner accès à ces données à des laboratoires de recherche afin qu'ils effectuent des analyses sans le risque que les données personnelles des participants soient divulguées.

En juin 2021, la revue *Nature* publiait un article intitulé « *comment les scientifiques adoptent les NFTs ?*⁷⁰ », en se demandant si cette tendance est « *une mode artistique fascinante, une catastrophe environnementale ou l'avenir de la génomique monétisée ?*⁷¹ » Si personne n'a encore de réponse aujourd'hui, la question est dorénavant posée.

70 « How scientists are embracing NFTs is a trend of auctioning non-fungible tokens based on scientific data a fascinating art fad, an environmental disaster or the future of monetized genomics ? », Nicola Jones, *Nature*, June 18, 2021, <https://www.nature.com/articles/d41586-021-01642-3>

71 *Ibid.*



ENJEUX ET QUESTIONS

Il n'aura fallu que trente ans pour profondément transformer la pensée libertarienne de l'invention d'internet et du web, et pour que le rêve initial de Norbert Wiener, J.C.R. Licklider, Robert Taylor et bien d'autres – créer un outil citoyen de participation active et de créativité décuplée par l'interaction – engendre une concentration sans précédent des services du web par quelques géants du numérique dont le modèle d'affaire repose sur l'exploitation des données personnelles des individus, nouveau pétrole du 21^e siècle.

La promesse d'une nouvelle décentralisation du web, portée par le web 3.0 et ses services reposant sur des blockchains, n'est-elle qu'une redistribution des cartes vers de nouveaux centres de pouvoir ? Comment assurer une réelle décentralisation des services comme l'hébergement d'applications et de données ?

Suite à notre analyse, nous constatons que les initiatives à l'œuvre dans le domaine des médias et de l'information politique n'ont rien donné de concluant. De plus, les initiatives dans le domaine de la science décentralisée sont encore au stade de l'expérimentation.

La vague des NFT* dans les industries culturelles augure-t-elle un rééquilibrage des rapports de force entre les artistes et les intermédiaires dont ils dépendent dans leur relation avec leur audience ? De quelle manière ces projets redistribuent la valeur entre les membres d'une communauté comme celle portée par Hive ou Steem ?

La question de la monétisation et de la propriété de contenus *via* NFT* ne rend-elle pas leur accès plus limité et restreint à un cercle d'initiés ? En quoi les NFT* permettraient-ils l'accès du plus grand nombre à l'art et à de nouvelles sources de financement ? Autant de questions qui n'ont encore pas de réponse aujourd'hui...

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 publié 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