SANTÉ

SEPTEMBRE 2022

WWW.BLOCKCHAINFORGOOD.FR

BLOCKCHAIN @POLYTECHNIQUE

bpifrance SERVIR L'AVENIR

Caisse des Dépôts GROUPE

INSTITUT Louis Bachelier

PB PositiveBlockchain.io

A PROPOS

BLOCKCHAIN FOR GOOD

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

NOS PARTENAIRES

BLOCKCHAIN @POLYTECHNIQUE

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

Caisse des Dépôts GROUPE

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

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

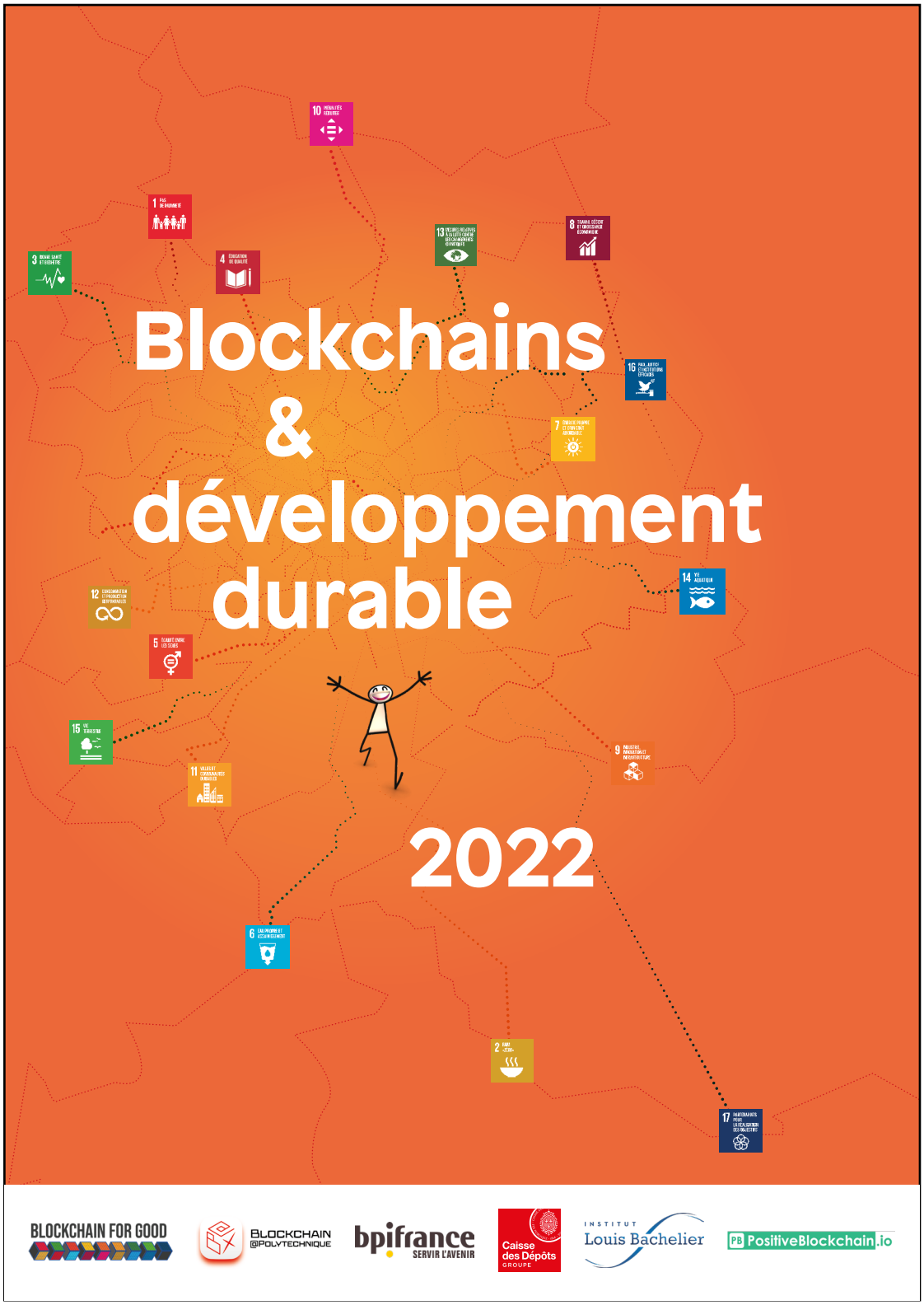
Bpifrance finance les entreprises - à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi leur activité export à travers une large gamme de produits. Conseil, université,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

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

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

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

CE CAHIER EST UN EXTRAIT DU RAPPORT :



LIBREMENT TELECHARGEABLE SUR BLOCKCHAINFORGOOD.FR

AUTEURS

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

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

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

CONTRIBUTEURS

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

RELECTEURS - CAHIER SANTÉ

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

TABLE DES MATIÈRES

SANTÉ

Nombre de projets dans la base : 148

Nombre de projets actifs : 71

Nom des projets actifs : Aenco ; Amchart ; Astri ; Avyantra ; Betterpath ; BitMark ; BlockMedx ; Bowhead Health ; BurstIQ ; CareChain ; Change Healthcare ; Citizen Health - Citizen DAO ; ConsilX ; CoverUS ; dClinic ; Decent (healthcare) ; DNAtix ; Doc.ai ; Embleema ; Encrypgen ; Factom ; «FarmaTrust» ; Gainfy ; Genecoin ; Geneyx ; GenoBank ; Grapevine ; Guardtime & Estonia eHealth strategy ; Hashed Health ; Health Verity ; Health Wizz ; Healthcoin.nl ; HIE of One ; HIT Foundation ; Humanscape ; intiva ; Iryo ; iSolve ; Kidner ; KimboCare ; Longenesis ; lunaDNA ; Lynx ; MediBloc ; MedicalChain ; MediLedger ; Meditect ; Medrec ; Medvice ; «MedX Protocol» ; Modum ; Molecule ; MyHealthMyData ; Nano Health ; Nebula Genomics ; Open Health Network ; Patientory ; Peer Ledger ; PharmaTrace ; PointNurse ; PPPHealth4All ; Prescrypto ; Quanti Health ; Ribbon blockchain ; Shivom ; Sicpa - Covid pass ; SkyChain Global ; Spiritus ; Statwig ; Zenome ; *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/

Les industries de santé, qui regroupent les acteurs de l'industrie pharmaceutique, les biotechs, les medtechs ainsi que les acteurs de la santé publique et de la santé se sont emparés du numérique à travers six grands chantiers, que la Fondation de l'Avenir décrit ainsi[1] : « **Les systèmes d'information en santé** permettant une meilleure coordination des soins *au sein d'un établissement de santé (Systèmes d'information Hospitalier ou SIH, Dossier Patient Informatisé ou DPI, etc.) ou d'un territoire de soins (Systèmes d'Information partagé de santé).* ***La télémédecine*** *offrant des possibilités de soins à distance : la téléconsultation, la téléexpertise, la télésurveillance, la téléassistance, et la régulation médicale.* ***La télésanté*** *intégrant des services de suivi et de prévention des individus dans un objectif principal de bien-être (objets connectés, applications mobiles d'auto-mesure, plateforme web, …).* ***Les dispositifs technologiques centrés patient ou grand public*** *: m-health ou m-santé (M pour Mobile) applications de santé mobiles, applications de santé web, objets connectés, réseaux sociaux (communautés de patients), portail d'information de santé, etc.*

1 Fondation de l'Avenir, Fondation pour la recherche médicale appliquée, reconnue d'utilité publique.

Les dispositifs technologiques centrés offreurs de soins tels les établissements de santé et les professionnels de santé *: les SIH internes, systèmes d'information partagés, systèmes d'information embarqué (ex : SMUR), dispositifs de télémédecine, etc.* ***Les dispositifs technologiques centrés acteurs assurantiels, régulateurs publics et industriels*** *: outils génériques de la gestion de la relation client (CRM) ainsi que ceux du* datamining *(données internes) ou du* big data *(données externes) permettant la collecte, le stockage et le traitement algorithmique de données massives de santé* ».

Cependant, l'écrasante majorité des systèmes d'information utilisés par l'ensemble de ces acteurs ne sont pas interopérables et les données des patients sont centralisées et répliquées au sein de chaque établissement, recopiées à nouveau dans chacun des systèmes d'information qui en demandent la transmission, et sont même parfois à nouveau rassemblées dans des méga plateformes comme le « Health Data Hub » en France, déployé en 2021[2], qui pose clairement des problèmes de souveraineté lorsque l'on sait que le prestataire d'hébergement est américain[3]. Or les données de santé sont par nature à caractère personnel, et sont dites « **données sensibles** » parce qu'elles révèlent des informations liées à la santé d'une personne.

L'usage de registres distribués de type blockchain permettrait, selon leurs promoteurs, d'assurer une meilleure interaction des organisations de santé avec un ou des systèmes d'identités décentralisées plutôt que des données personnelles (voir Chapitre Identité et propriété), ce qui aurait pour conséquence **la réappropriation de ses données de santé par le patient**, à propos desquelles il décide du partage et surtout, l'assurance de la confidentialité de ses données de santé ou tout du moins l'assurance d'être celui qui autorise ou refuse l'utilisation de ses données personnelles par des tiers. (*Si les données des patients des hôpitaux n'étaient pas administrées en silo par chaque établissement, les rançongiciels et cyberattaques perdraient considérablement d'intérêt).*

L'usage de registres distribués permettrait également de considérablement améliorer **l'accès aux données de santé entre des parties prenantes disparates**, présentant parfois des intérêts contradictoires. La mise en place de tels registres permettrait en outre une réduction des coûts de soins de santé, par la rationalisation et l'optimisation des processus opérationnels, administratifs et financiers.

2 La totalité des données de santé des Français va bien être hébergée en France, mais par un opérateur américain, lequel en vertu du *Cloud Act* pourra être contraint par la justice américaine de transférer toutes ces informations personnelles aux États-Unis. « Le grand écart entre Gaia-X et le Health Data Hub », Jacques-André Fines Schlumberger, *La revue européenne des médias et du numérique* - N°54bis-55 Automne 2020, https://la-rem.eu/2020/12/le-grand-ecart-entre-gaia-x-et-le-health-data-hub/

3 « Le grand écart entre Gaia-X et le Health Data Hub », Jacques-André Fines Schlumberger *La revue européenne des médias et du numérique* - N°54bis-55 Automne 2020, https://la-rem.eu/2020/12/le-grand-ecart-entre-gaia-x-et-le-health-data-hub/

Les 148 initiatives blockchain que nous avons identifiées dans le domaine de la santé s'organisent ainsi autour de ces promesses, mais quelque dix ans après le lancement des premiers projets, force est de constater que beaucoup ont disparu, (77 projets sur 144 ne sont plus actifs), que d'autres n'ont de blockchain que le nom. Il ne subsiste, au final, que quelques cas d'usages parmi les 71 projets blockchain actifs référencés au sein de l'annuaire PositiveBlockchain.io.

Pour Anca Petre, fondatrice de 23 Consulting, « *les projets n'aboutissent pas car ils nécessitent de travailler en consortium. C'est le fondement même de la technologie, mais cela pose des questions de propriété intellectuelle, de modèle économique, de gouvernance, sans compter les questions réglementaires*[4] ». Les blockchains, dans le domaine de la santé, mettent en lumière que **les enjeux auxquels sont confrontées les organisations et les patients sont d'abord des enjeux politiques et de moins en moins des enjeux techniques**. Et Anca Petre de souligner « *la technologie n'est plus un sujet, elle est maîtrisée. Idem pour les cas d'usage. Ce sont la gouvernance et la mise en œuvre qui posent problème aujourd'hui* ». En janvier 2021, une étude[5] menée par des chercheurs de SingHealth Polyclinics à Singapour n'a identifié que dix projets blockchain opérationnels dans le domaine de la santé parmi les 8 326 blockchains publiques référencées sur le site coinmarketcap.com.

Une entreprise de santé qui lancerait seule une blockchain n'a aucun sens. Un consortium d'entreprises du domaine de la santé qui exploiterait une blockchain publique commune en a plus. Dans ce sens, **PharmaLedger,** en réunissant 29 organisations du domaine de la santé, est une initiative prometteuse[6]. Mais un méga consortium d'entreprises de santé qui s'appuierait tout à la fois sur un système d'identités décentralisées, sur des blockchains publiques et des *sidechains** privées n'existe pas encore.

Toutefois, si la mise en œuvre de registres distribués appliquée au domaine de la santé n'en est encore qu'à ses débuts, les expérimentations et projets pilotes menés depuis 2010, ainsi qu'un certain engouement de la part de la communauté scientifique donne à voir quatre grands terrain d'expérimentation :

4 « Blockchain dans la pharma: les promesses s'envolent, les cas d'usage restent », Léo Caravagna, TicPharma, 5 janvier 2021, ticpharma.com.

5 « Commercially Successful Blockchain Healthcare Projects: A Scoping Review. », Fang, H. S. A, Blockchain *in Healthcare Today*, *4*. 2021, https://doi.org/10.30953/bhty.v4.166

6 Parrainé par l'Initiative en matière de médicaments innovants (IMI) et la Fédération européenne d'associations et d'industries pharmaceutiques (EFPIA) dans le cadre du programme Horizon 2020, PharmaLedger est un projet de 36 mois, débuté en 2020, qui réunit 12 entreprises pharmaceutiques mondiales et 17 entités publiques et privées, notamment des organismes techniques, juridiques et réglementaires, des universités, des organismes de recherche et des organisations représentant les patients.

1. La gestion des données de santé et des dossiers médicaux des patients, appelée « dossier médical partagé » (DMP) en France, ou Electronic Health Records (EHRs) ailleurs dans le monde, des Etats-Unis au Brésil en passant par la Chine, le Danemark ou encore l'Inde.
2. La recherche sur de nouveaux médicaments, les essais cliniques, et la médecine de dite précision.
3. L'amélioration de la traçabilité des médicaments.
4. L'optimisation de la couverture de l'assurance maladie, notamment par l'usage de *smart contracts**.

Selon la manière dont ils sont conçus, ces projets s'inscrivent dans la poursuite de l'Objectif de développement durable 3, qui vise « *assurer la santé et le bien-être de tous, en améliorant la santé procréative, maternelle et infantile, en réduisant les principales maladies transmissibles, non transmissibles, environnementales et mentales. Ces enjeux sanitaires pourront être réalisés à condition de mettre en place des systèmes de prévention visant la réduction des comportements déviants ainsi que tout facteur de risque pour la santé, d'assurer un accès universel à une couverture médicale et aux services de santé, de soutenir la recherche et le développement de vaccins et de médicaments et améliorer la gestion des risques sanitaires dans les pays en développement*[7] ».

Selon le Programme des Nations Unies pour le Développement (PNUD), « *400 millions de personnes n'ont pas accès à des services de santé de base, 40% de la population mondiale n'a pas de protection sociale, et 1,6 milliard de personnes vivent dans des environnements fragiles où le manque d'accès aux services de santé basiques représente un obstacle majeur*[8] ».

La cible 3.8 vise explicitement à faire en sorte que « *chacun bénéficie d'une couverture sanitaire universelle, comprenant une protection contre les risques financiers et donnant accès à des services de santé essentiels de qualité et à des médicaments et vaccins essentiels sûrs, efficaces, de qualité et d'un coût abordable*[9] ». La cible 3.b entend, quant à elle, « *appuyer la recherche et la mise au point de vaccins et de médicaments contre les maladies, transmissibles ou non, qui touchent principalement les habitants des pays en développement, donner accès, à un coût abordable, à des médicaments et vaccins essentiels (...)*[10] ».

7 Objectif de développement durable 3 : Donner aux individus les moyens de vivre une vie saine et promouvoir le bien-être à tous les âges, Ministère de la Transition écologique, https://www.agenda-2030.fr/17-objectifs-de-developpement-durable/article/odd3-donner-aux-individus-les-moyens-de-vivre-une-vie-saine-et-promouvoir-le

8 Programme des Nations Unies pour le développement, Objectif de développement durable 3 : Bonne santé et bien-être, https://www.agenda-2030.fr/17-objectifs-de-developpement-durable/article/odd3-donner-aux-individus-les-moyens-de-vivre-une-vie-saine-et-promouvoir-le

9 *Ibid.*

10 *Ibid.*

Voici quelques initiatives blockchain à l'œuvre dans les domaines de la gestion de données de santé, la recherche et la traçabilité des médicaments.

Données de patients

Dans le système de santé actuel, les patients disséminent leurs données personnelles à chaque fois qu'ils interagissent avec un acteur du système de santé, - hôpitaux, pharmacies, réseaux, médecins etc. Même si les données de santé, par nature à caractère personnel, sont dites **données sensibles** parce qu'elles révèlent des informations liées à la santé d'une personne, le modèle qui consiste à centraliser les données, en interne sur des serveurs ou bien dans des services d'hébergement à distance est devenue la norme. Or les données de santé sont intimement liées à la notion d'identité numérique (voir chapitre Identité et propriété) et plus précisément, à la notion d'identité numérique décentralisée, portée par les technologies des registres distribués et la normalisation de standards techniques portée notamment par le W3C.

En 2009, en même temps que Satoshi Nakamoto diffusait la première version du logiciel Bitcoin sur le site P2P Foundation[11], Catherine Quantin, alors au Service de Biostatistique et d'Informatique Médicale du Centre Hospitalier Régional et Universitaire de Dijon, en France, s'inquiétait déjà ainsi :

« Le fait que toutes les informations soient contenues en un seul lieu est un rêve qui témoigne d'une vision ancienne de l'organisation où le centralisme était la voie unique qu'il soit inspiré du jacobinisme à la française ou du centralisme démocratique cher aux partisans des systèmes collectivistes. Il y a pourtant plusieurs décennies que les pouvoirs publics ont pris conscience **du danger intrinsèquement lié à cette organisation centrale qui expose à tout perdre si elle est détruite**. Comment ne pas imaginer que tous les *hackers* du monde prendraient comme un défi le fait de s'introduire dans la banque nationale des dossiers médicaux des patients pour les consulter ou pire changer les informations qu'ils contiennent ? Comment ne pas craindre que des terroristes de toutes convictions pourraient y voir une chance extraordinaire de déstabiliser tout un pays en s'attaquant à un domaine auquel les citoyens accordent une importance majeure : leur santé et la confidentialité des informations qui s'y rattachent ? Comment accepter le risque que fait courir une telle organisation pour la vie privée et la sécurité des personnes si l'État qui l'a mis en place s'écartait des voies de la démocratie et du respect des libertés individuelles[12] ».

11 P2P Foundation Forum Posts https://www.bitcoin.com/satoshi-archive/forum/p2p-foundation/#selection-13.1-2.3

12 « Gestion décentralisée des documents médicaux des patients. Un système de recherche et d'accès aux

L'apport fondamental des blockchains dans le domaine de l'identité numérique, et donc des données de santé, est d'**inverser le modèle actuel fondé sur la centralisation des données gérée par une organisation, vers un modèle fondé sur la vérifiabilité d'attestations contrôlées par une personne**. Alors que le modèle actuel donne tout pouvoir à l'organisation qui « gère » les données de santé des individus, le modèle de l'identité numérique décentralisée redonne à l'individu l'opportunité de décider qui accède à ses informations personnelles.

Ce qui, finalement, correspond à l'esprit même du Règlement général sur la protection des données (RGPD) applicable dans l'ensemble des 27 États membres de l'Union européenne depuis le 25 mai 2018 et qui pose, entre autres, les principes du consentement « explicite » et « positif » d'une personne quant à l'usage de ses données personnelles ainsi que du droit à l'effacement de ces mêmes données. Ce changement de paradigme permet également à des tiers d'accéder aux données de santé des personnes tout en ayant la garantie de leur confidentialité et de l'usage qui en est fait.

La promesse d'initiatives blockchain consiste à rendre aux patients le contrôle de leurs données personnelles de santé. **Medical Chain,** créé en 2017 à Londres en Grande-Bretagne, affirme développer un système « *qui donne aux utilisateurs finaux du monde entier une plateforme sécurisée pour gérer et transférer leurs données de santé, afin d'obtenir des informations exploitables pour améliorer résultats de santé et de bien-être* ». **Patientory**, fondée en 2015 à Atlanta aux Etats-Unis promet de « *donner au patient le contrôle de ses données médicales, en leur donnant le pouvoir de partager la version la plus exhaustive et la plus complète de son dossier, avec chaque organisation de son réseau médical* ».

My Health My Data, un consortium européen d'une quinzaine de partenaires, subventionné à hauteur de 4 millions d'euros dans le cadre du programme européen Horizon 2020 entre 2016 et 2019 a eu pour ambition de « sé*curiser les données des patients, de réduire* » par conception » *le risque d'usurpation d'identité et d'atteinte à la vie privée, et d'introduire une nouvelle façon de partager les informations privées en responsabilisant leurs principaux propriétaires, les patients*[13] ». Filiale du groupe Be-ys, la société française Be-Studys[14] commercialise **ProRegister** depuis août 2021 une

données », Quantin Catherine, Coatrieux Gouenou, Fassa Maniane *et al.*, *Document numérique*, 2009/3 (Vol. 12), p.23-35, https://www.cairn.info/revue-document-numerique-2009-3-page-23.htm

13 « My Health - My Data », European Commission, retrieved May 16, 2022, https://cordis.europa.eu/project/id/732907

14 « Be-studys veut associer les patients à la recherche médicale », Sylvie Jolivet, *Les Echos*, 9 mai 2019, https://www.lesechos.fr/pme-regions/innovateurs/be-studys-veut-associer-les-patients-a-la-recherche-medicale-1017207

version « *industrialisée du pilote 'My health, my data'* », actuellement utilisé par quatre hôpitaux européens à Rome, Berlin et Londres et qui gère les données de santé de 81.000 patients. David Manset, directeur général de Be-studys explique plus en détail le projet ainsi : « *Les établissements de santé sont équipés d'un logiciel pour mettre à disposition les données des patients qui donnent leur consentement. Ce logiciel indexe et pseudonymise les données. Il crée une* 'carte d'identité' *de la donnée et l'enregistre dans la blockchain, qui ne contient pas de données personnelles* (...) *Chaque fournisseur de données est considéré comme un tiers de confiance. La blockchain permet de référencer leurs données sans être en conflit avec le RGPD. L'accès aux données se fait via le portail 'My health, my data'. La demande d'accès créé un smart contract* qui permet la mise à disposition des données et la traçabilité de toutes les opérations* via *une API*[15] ».

Cependant, la plupart de ces initiatives, reposant sur des blockchains privées, la plupart du temps avec permission, relèvent plus de l'amélioration et de l'optimisation des systèmes existants plutôt que de nouveaux modèles réellement décentralisés où les individus ont l'entière maîtrise de leurs données de santé. Des projets de blockchains publiques dans le domaine de la santé qui s'adressent à tout un écosystème ou un domaine spécifique sont complexes à mettre en place, principalement en raison de la diversité des acteurs et de leurs intérêts parfois contradictoires.

Dans un tout autre domaine, **le séquençage du génome humain trouve de nombreuses applications en médecine, en biologie moléculaire, en génétique médicale, en microbiologie** afin de poser un diagnostic, d'identifier des mutations génétiques ou les prédispositions génétiques d'une personne pour certaines maladies. Alors que le projet Génome humain, *Human Genome Project*, premier séquençage du génome humain a été lancé en 1988, s'est achevé en 2003 et a coûté 2,7 milliards de dollars[16], un particulier peut aujourd'hui faire procéder au séquençage complet de son génome pour 100 dollars[17].

En 2015, des chercheurs ont estimé qu'entre 100 millions et 2 milliards de génomes humains pourraient être séquencés d'ici 2025[18].

15 « Blockchain dans la pharma: les promesses s'envolent, les cas d'usage restent », Ticpharma, retrieved May 16, 2022, https://www.ticpharma.com/story/1498/blockchain-dans-la-pharma-les-promesses-s-envolent-les-cas-d-usage-restent.html ?search=MHMD

16 « Business, éthique, légalité... Le séquençage de l'ADN en questions », Alexandre Léchenet, *Le Monde*, 18 août 2014, https://www.lemonde.fr/les-decodeurs/article/2014/08/18/le-sequencage-du-genome-comment-ca-marche_4472313_4355770.html

17 « Une biotech chinoise lance le premier test génétique à 100 dollars », Fabrice Delaye, 27 février 2020, Heidi.news, heidi.news/

18 « Big Data: Astronomical or Genomical ? », Stephens ZD, Lee SY, Faghri F, Campbell RH, Zhai C, Efron MJ, et al., PLoS Biol, 2015, https://doi.org/10.1371/journal.pbio.1002195

Mais « *qui a accès aux données et comment assurer leur sécurité ? Comment les données peuvent-elles être utilisées et partagées de manière responsable sans perdre les avantages du partage pour la recherche et les (futurs) patients ?*[19] » s'interroge Mohammed Alghazwi, chercheur à l'Université de Groningen aux Pays-Bas.

La société 23andMe illustre parfaitement l'écueil de la centralisation des données de santé des individus par une seule entité. Créée en 2006 en Californie, 23andMe est une société de biotechnologie américaine qui propose aux particuliers une analyse de leur code génétique.

En 2018, la *startup* a ouvert son capital à l'entreprise de santé GlaxoSmithKline[20], à hauteur de 300 millions de dollars, en autorisant également le géant pharmaceutique à mettre la main sur les données génomiques personnelles de ses clients « à des fins de recherches médicales pour développer de nouveaux médicaments[21] ». Nul ne sait ce qu'il est depuis advenu, si des données ont fuité et de quelle manière les données génétiques des clients de 23andMe ont été utilisées par GlaxoSmithKline. Une chose est sûre, c'est qu'aucun des « clients » de l'entreprise n'a pu s'opposer à l'utilisation de leurs données de santé par le géant pharmaceutique.

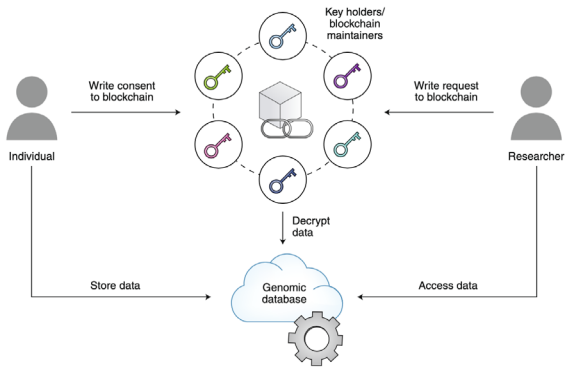
La nature même de ces services, qui consistent à confier des données génomiques personnelles à une seule entité qui gère les données de manière centralisée, est une pratique de plus en plus risquée. Aux Etats-Unis, sur la seule année 2021, plus de 40 millions de dossiers médicaux ont été publiquement exposés[22]. Et le législateur sera toujours en retard et les risques d'attaques informatiques gagneront toujours en intensité. Robert Kain, co-fondateur de Luna DNA Inc[23], une plate-forme communautaire de recherche sur la santé et l'ADN explique ainsi qu'aux Etats-Unis, « *la loi sur la non-discrimination en matière d'informations génétiques protège les individus contre la discrimination de la part des employeurs et des compagnies d'assurance maladie. Mais, elle ne s'applique pas à l'assurance-vie et à l'assurance-invalidité, et ne protège pas contre la discrimination dans d'autres domaines, tels que l'éducation et le logement. À l'avenir, d'autres utilisations des données génomiques, potentiellement inquiétantes, pourraient être développées.*

19 Alghazwi, M., Turkmen, F., Velde, J. V. D., & Karastoyanova, D. (2021). Blockchain for Genomics: A Systematic Literature Review. arXiv. https://arxiv.org/pdf/2111.10153
20 « 23andMe and Other Sites are Selling Users' Genetic Data: How Safe is Your DNA ? », Justin Roberti, February 28, 2021, https://hackernoon.com/23andme-and-ancestrycom-are-selling-users-genetic-data-how-safe-is-your-dna-x64k3330
21 « A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned ? », Jamie Ducharme, Time, Jul 26 2018, https://time.com/5349896/23andme-glaxo-smith-kline/
22 « The biggest healthcare data breaches of 2021 », Kat Jercich, November 16, https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021
23 « Database shares that transform research subjects into partners. », Kain, R., Kahn, S., Thompson, D. *et al.*, *Nat Biotechnology* 37, 1112–1115, 2019, https://doi.org/10.1038/s41587-019-0278-9

Par exemple, les données génomiques personnelles pourraient devenir précieuses pour la publicité ciblée ».

Encrypgen[24], **Zenome**[25], **DNAtix**[26], ou encore **Nebula Genomics** sont quelques-unes de ces *startups* proposant un modèle alternatif à celui d'entreprises privées comme 23andMe et proposent à l'utilisateur de garder le contrôle de ses données génomiques, et même d'en tirer profit s'il souhaite les partager avec des acteurs de la santé. **Nebula Genomics**, créé en 2016 par Dawn Song à San Francisco aux Etats-Unis, est une entreprise de biotechnologie qui offre aux particuliers un séquençage de leur génome dont les données sont indéchiffrables pour un tiers et donne à leur client le contrôle de qui peut y accéder, selon les finalités qu'il choisit, révoque et recompose.

La *startup* s'appuie sur Oasis Labs qui développe le réseau Oasis[27] (ROSE), fondé par Dimitar Dimitrakiev, Phillipp Grenzebach et Jeremias Grenzebach en mars 2017 aux Pays-Bas. Le réseau Oasis (ROSE) est une blockchain de premier niveau, basée sur la blockchain Cosmos (ATOM), axée sur la protection de la vie privée et dont le mécanisme de consensus repose sur la preuve



de détention*. L'accès aux données génomiques est « *contrôlé par plusieurs parties indépendantes qui détiennent des fragments d'une clé de cryptage partagée. De plus, ces parties maintiennent une blockchain qui stocke de manière immuable et transparente les demandes d'accès aux données et le consentement des utilisateurs*[28] ». Le réseau Oasis est construit pour la finance ouverte et l'économie de données vérifiables à l'aide du SDK* Cosmos, dont l'architecture est similaire à la structure des blockchains publiques **Avalanche** ou **Polkadot**, reliant plusieurs blockchains différentes au sein d'un même écosystème. Nebula Genomics utilise le réseau Oasis Labs pour sécuriser les données de ses clients, et ainsi leur en donner le contrôle[29].

Zenome, créé à Moscou en Russie en 2017, utilise la blockchain publique Ethereum et des *smart contracts** pour mettre en relation des personnes

24 Fondée à New York aux Etats-Unis en 2016.
25 Fondée à Moscou en Russie en 2017.
26 Fondée à Ramat Gan en Israël en 2018.
27 « Ensuring auditability and immutability of actions with a distributed network. », Oasis Labs, retrieved 16 May, 2022, oasislabs.com
28 « Data privacy in the age of personal genomics », Kain, R., Kahn, S., Thompson, D. *et al.*, Database shares that transform research subjects into partners, *Nat Biotechnology* 37, 1112–1115, 2019, https://doi.org/10.1038/s41587-019-0278-9 .
29 « Take Control of your Genomic Data », Nebula Genomics, retrieved May 16, 2022, nebula.org

souhaitant partager et vendre le séquençage de leur génome auprès de tiers, dont notamment des chercheurs. Le service proposé par Zenome est double : d'une part, il permet à quiconque de fournir les ressources de son ordinateur, que ce soit de l'espace disque ou du temps de processeur, pour le besoin de stockage distribué et l'analyse de données génétiques et obtenir une récompense en token ZNA et de l'autre, assurer une sécurisation des données génomiques des utilisateurs de son service.

A côté de l'offre de ces *startups*, des applications non commerciales de recherche génomique fournissent des solutions pour « *le partage, le traitement/ analyse, le stockage sécurisé, le contrôle d'accès et la journalisation des accès aux données génomiques*[30] » en s'appuyant sur les caractéristiques intrinsèques des blockchains, « *l'immuabilité, la décentralisation et le contrôle de l'accès/ de l'utilisation*[31] ».

Selon l'étude « *Blockchain for Genomics: A Systematic Literature Review*[32] » publiée en novembre 2021, source de l'image ci-dessous, sur les treize entreprises commerciales identifiées par les chercheurs, la majorité des registres distribués repose sur des blockchains privées avec permissions, dont 31 % sont développés sur Multichain[33] et 27,6 % sur la blockchain publique Ethereum (voir graphique *infra*).

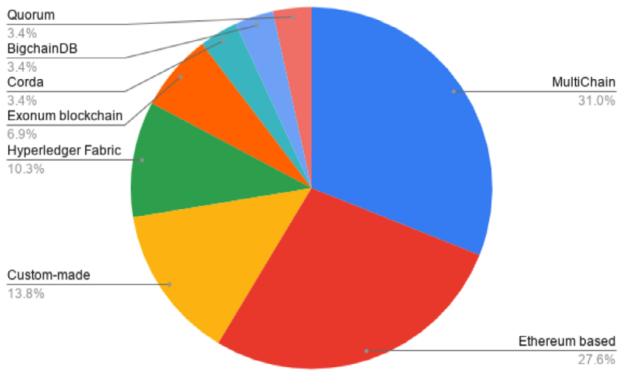


Fig. 8. Blockchain platforms used in genomic data applications

30 « Blockchain for Genomics: A Systematic Literature Review. », Alghazwi, M., Turkmen, F., van der Velde, J., & Karastoyanova, D., 2021, https://arxiv.org/pdf/2111.10153.pdf.
31 *Ibid.*
32 *Ibid.*
33 MultiChain est une plateforme blockchain permettant de construire et de déployer des réseaux blockchain privés ou avec permission. MultiChain est une source ouverte sous la licence GPLv3, disponible sur Github, et offre également des licences commerciales et un support. « MultiChain For Developers », Multichain, retrieved May 16, 2021, https://www.multichain.com/developers/

Recherche et essais cliniques

Le rapport « *Blockchain technology applications in healthcare: An overview* », publié par des chercheurs Indiens en septembre 2021, estime que, dans le domaine des essais clinique et de la recherche, les blockchains pourraient « *résoudre les problèmes de modification des résultats et de fouille des données, assurer le transfert de rapports et de résultats d'essais cliniques permanents et horodatés, réduisant ainsi les cas d'escroquerie et d'erreur dans les essais cliniques, et résoudre les problèmes de faux résultats*[34] ».

D'autant plus que les essais cliniques menés pour la mise au point de nouveaux médicaments s'appuient de plus en plus sur le numérique, transition accélérée par la pandémie mondiale de Covid-19, pour notamment, selon le site d'information professionnelle mind Health, « *réduire les délais de recrutement des patients, ouvrir l'accès aux essais cliniques à un plus grand nombre d'entre eux, faciliter le recueil du consentement mais aussi simplifier la conduite des essais, fidéliser les patients dans l'étude ou encore utiliser des logiciels et outils numériques pour améliorer la supervision des études…, les usages se multiplient et contribuent au développement des essais décentralisés*[35] ».

Les professionnels de la santé parlent dorénavant « d'*essais cliniques décentralisés* », ou de « *données de santé en vie réelle* », c'est-à-dire que les participants à une un essai clinique ne se déplacent plus physiquement au sein de centres de recherche mais sont suivis à distance avec, éventuellement, le déplacement chez un professionnel de santé local ou même directement chez eux.

La start-up franco-américaine **Embleema Health Network** développe depuis 2018 plusieurs services reposant sur un registre distribué pour partager des données de santé pour la recherche contre les maladies chroniques et les maladies rares, en rassemblant patients, communautés médicales, scientifiques, industriels et autorités de santé. L'outil informatique d'Embleema permet notamment de gérer le consentement des patients quant au partage de leurs données de santé, afin qu'ils puissent participer à des essais cliniques rémunérés. D'un point de vue technique, Embleema a développé sur Hyperledger Fabric une blockchain privée avec permission dont tous les nœuds sont gérés par l'entreprise.

Elle travaille aujourd'hui pour la Food and Drug Administration (FDA) aux Etats-Unis, l'administration américaine

34 « Blockchain technology applications in healthcare: An overview. », Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab, International Journal of Intelligent Networks, Volume 2, 2021, Pages 130-139, https://doi.org/10.1016/j.ijin.2021.09.005.

35 Mind Health est un service d'information professionnelle consacré à la mutation des industries de santé, édité par Frontline MEDIA, qui bénéficie du soutien de la Région Île-de-France, dans le cadre du programme PM'up, et de L'Institut pour le Financement du Cinéma et des Industries Culturelles (IFCIC), « Présentation de Mind Health », Mind Health, consulté le 16 mai 2020, https://www.mindhealth.fr/presentation/

chargée d'autoriser la commercialisation des médicaments sur le territoire. Dans des propos rapportés par mind Health, Robert Chu, le fondateur d'Embleema explique l'objet de ce contrat de six millions de dollars sur trois ans : « *Il s'agit de constituer une base de données de recherche comprenant toutes les informations génomiques annotées des variants du covid-19 et d'une manière générale, de tous les variants des pathogènes (influenza, grippe, HIV, hépatite B, salmonelle). À travers la plateforme Embleema, la FDA partagera ces données avec l'ensemble des chercheurs dans le monde. Lorsqu'un laboratoire pharmaceutique utilise une donnée de référence sur notre plateforme, la FDA sait qu'elle est de qualité réglementaire et qu'elle répond à des critères de qualité élevés qui comprennent la provenance, l'auditabilité de tous les traitements réalisés dessus. Tout le* pipeline *de traitement de la donnée doit se conformer au maximum aux standards internationaux. Nos algorithmes permettent de garantir une véracité dans l'analyse. En plus d'éviter les fraudes ou la falsification, notre système accélère l'approbation réglementaire des produits de santé relatifs à tous ces pathogènes et leur mise à disposition aux patients*[36] ».

Il n'empêche qu'une blockchain privée avec autorisation et dont tous les nœuds sont gérés par une seule entreprise correspond plus à l'optimisation d'interactions sur une base de données plutôt qu'à la mise en œuvre d'un langage commun universel permettant tout à la fois de garantir la confidentialité des données des personnes et permettre le traitement en masse de ces mêmes données de santé. Ce processus a néanmoins le mérite d'optimiser une collecte « *coûteuse, lente et manuelle, monétisée par des intermédiaires* » expliquait Alexis Normand en 2018, alors en charge du consortium chez Embleema, en citant l'exemple du coût de la reconstitution d'un dossier médical complet d'une personne atteinte de mucoviscidose, qui s'élève à 10 000 dollars, ou de la maladie de Parkinson, qui s'élève à 20 000 dollars[37].

ConsilX, créée en 2017 à Singapour, avec un bureau en Inde, se présente également comme une plateforme « d'*essais cliniques décentralisés*[38] », reposant sur des « *données de santé en vie réelle* ». La plateforme, appelée LifeLedger™, articulerait une solution de « consentement numérique », activable sur place ou à distance, des dispositifs de mesures de données de santé, à porter par le patient, ainsi que des journaux électroniques et des questionnaires, un module de télémédecine pour assurer une communication entre médecins et patients, le tout géré par une blockchain

36 « Un essai clinique totalement virtuel est cent fois plus rapide qu'une étude classique », Robert Chu (Embleema) », Camille Boivigny, Mindhealth, 18 octobre 2022, https://www.mindhealth.fr/parcours-de-soins/robert-chu-embleema-un-essai-clinique-totalement-virtuel-est-cent-fois-plus-rapide-quune-etude-classique/
37 « Embleema met la blockchain au service de la pharmacovigilance », Wassinia Zirar, TicPharma, 12 octobre 2018, https://www.ticpharma.com/story/732/
38 « Platform Features », Consilx, retrieved May 16, 2022, https://www.consilx.com/platforms-overview

et des *smart contracts** pour « notariser les données » et permettre au patient d'autoriser ou non à partager ses données de santé. Comme les autres projets, celui-ci met en œuvre une blockchain privée.

Molecule, créé à Berlin en Allemagne en 2018, est « *une place de marché pour le financement, la collaboration et la transaction de projets de recherche biopharmaceutique en phase de démarrage*[39] ».

Les chercheurs présentent leurs projets de recherche, trouvent des investisseurs et des collaborateurs et développent leurs projets de recherche. Les investisseurs et les fonds choisissent les projets de recherche biopharmaceutique et financent ceux retenant leur attention. L'infrastructure de la plateforme Molecule est construite sur Ethereum permettant aux chercheurs et aux investisseurs d'avoir un accès complet à l'écosystème de la Finance décentralisée (DeFi). Le catalogue des projets de recherche à financer est public[40].

Par exemple, le programme « *découvrir de nouveaux activateurs de l'autophagie*[41] » (l'autophagie est un processus d'auto-digestion qui consiste en une dégradation de composants intracellulaires par le lysosome) » porté par le professeur de biologie cellulaire moléculaire Viktor Korolchuk de l'Université de Newcastle en Angleterre a reçu 285 000 dollars de financement pour effectuer ses recherches. Est associé au projet de recherche des jetons non fongibles (NFT*) qui correspondent aux investissements et à l'exploitation des droits de propriété intellectuelle.

Paul Kohlhaas, co-fondateur de Molecule explique ainsi que cette nouvelle approche permet « *la combinaison jetons non fongibles (NFT), une nouvelle infrastructure d'échange automatique (AMM*) et des structures de gouvernance (DAO*) pour réinventer la propriété intellectuelle, le financement de ces actifs*[42] ». En juin 2022, Molecule référence 250 projets de recherche à financer, trois Organisations autonomes décentralisées (DAO*) rassemblant 4 500 personnes et capitalisant plus de 10 millions de dollars[43].

39 What is Molecule?: https://docs.molecule.to/documentation/introduction/what-is-molecule
40 Discover Research Projects Invest in biopharma researchers and their work https://discover.molecule.to
41 Discovering Novel Autophagy Activators https://discover.molecule.to/projects/cl3vghfw7005209lcesv415qq
42 An Open Bazaar for Drug Development: Molecule Protocol Paul Kohlhaas June 11, 2021 https://medium.com/molecule-blog/an-open-bazaar-for-drug-development-molecule-protocol-a47978dd914
43 Molecule: https://molecule.to/

Traçabilité des médicaments

Selon l'Organisation mondiale de la Santé (OMS), un médicament sur dix en circulation dans le monde est de « *qualité inférieure et falsifié*[44] », un sur quatre dans les pays en développement. La falsification de médicaments concerne dorénavant toutes les principales classes thérapeutiques, en ce y compris les médicaments, vaccins et produits de diagnostic *in vitro.* Toujours selon l'OMS, « *ce sont les pays à revenu faible ou intermédiaire, ceux dans des zones de conflits, de troubles civils et ceux dont les systèmes de santé sont faibles ou inexistants qui supportent la plus lourde part du problème des produits médicaux de qualité inférieure ou falsifiés*[45] ».

Plusieurs solutions ont déjà été imaginées par le passé pour lutter contre les médicaments falsifiés : l'impression d'un hologramme sur l'emballage d'un médicament, qui pourrait cependant être facilement contrefait ; la sérialisation de masse, *via* un système d'identification par radiofréquence (RFID) pour attribuer des identifiants uniques aux emballages, mais qui, en plus d'être coûteux, pourrait également être facilement contrefait ; les technologies de chiffrement de masse (*Mass encryption technology*), qui nécessitent toutefois que tous les acteurs utilisent la même technologie, ce qui semble compliqué à mettre en œuvre ; ou encore la directive de l'Union européenne sur les médicaments falsifiés (FMD) qui vise à rendre obligatoire, en Europe, l'identification des médicaments au fur et à mesure de leur progression sur toute la chaîne d'approvisionnement.

La communauté scientifique propose également des modèles et « solutions » blockchains pour lutter contre la contrefaçon de médicament, dont notamment, **LifeCrypter**[46], créé en 2017, **Drugledger**[47] en 2018 ou encore **PharmaCrypt**[48] en 2020. Tous présentent un registre distribué comme la réponse la plus appropriée aux problématiques des médicaments contrefaits et à leur traçabilité, du site de production jusqu'au patient :

Ces initiatives partent du constat qu'une autorité centralisée est un « point de défaillance unique », et proposent le développement de registres distribués assortis de *smart contracts** afin de garantir la transparence de ces chaînes logistiques complexes, parmi lesquelles **StaTwig** fondée à Hyderabad en Inde

44 « Produits médicaux de qualité inférieure ou falsifiés », WHO, retrieved May 16, 2022, https://www.who.int/fr/news-room/fact-sheets/detail/substandard-and-falsified-medical-products
45 *Ibid*.
46 « Blockchain technology in the pharmaceutical industry. », Schöner, M. M., Kourouklis, D., Sandner, P., Gonzalez, E., & Förster, J., 2017, Frankfurt, Germany: Frankfurt School Blockchain Center.
47 « Drugledger: A Practical Blockchain System for Drug Traceability and Regulation. », Huang, Yan & Wu, Jing & Long, Chengnian., Cybermatics, IEEE Explore, 2018, 10.1109/Cybermatics_2018.2018.00206.
48 « PharmaCrypt: Blockchain for Critical Pharmaceutical Industry to Counterfeit Drugs, », N. Saxena, I. Thomas, P. Gope, P. Burnap and N. Kumar, in *Computer*, vol. 53, no. 7, July 2020, pp. 29-44, doi: 10.1109/MC.2020.2989238

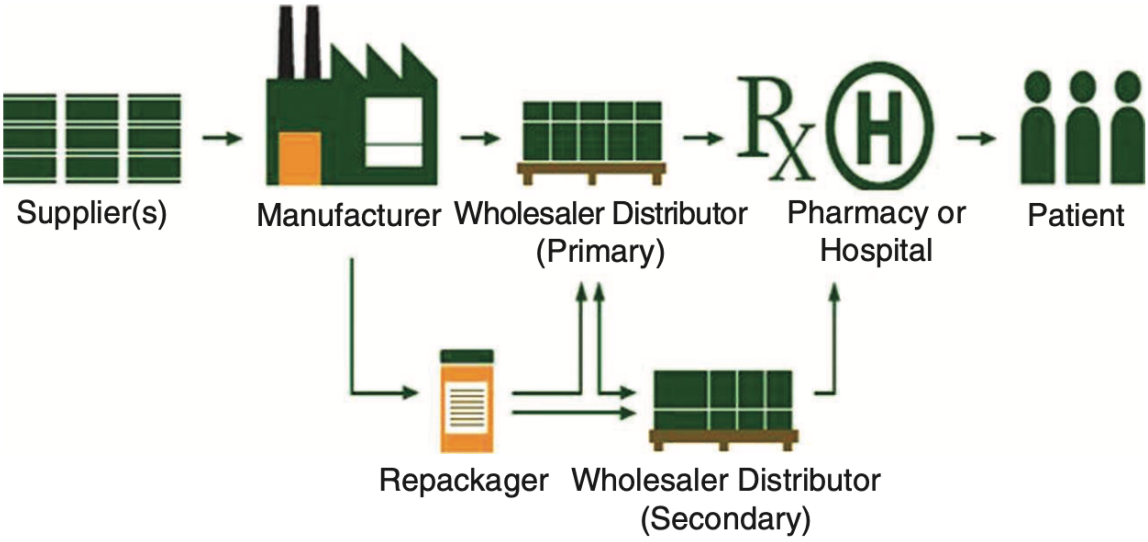
en 2016, **Meditect**, créée à Bordeaux en France en 2017, **Mediledger** créé à San Francisco en 2017 ou encore **PharmaTrace**, créé à Munich en Allemagne en 2017.

Mais beaucoup de ces initiatives consistent à développer des blockchains privées avec permission, ce qui prête à penser que le système mis en place permet essentiellement d'optimiser les échanges d'informations entre les parties prenantes sans véritablement garantir une véritable décentralisation, une immutabilité des données ainsi qu'un contrôle transparent de leur accès et de leur utilisation, portée par des blockchains publiques.

Meditect a développé une solution de traçabilité et d'authenticité des médicaments envoyés d'Europe vers l'Afrique en s'appuyant sur la directive européenne « Médicaments Falsifiés » en vigueur depuis février 2019. Initiée en 2011, cette directive européenne impose aux laboratoires pharmaceutiques d'inscrire sur chaque boîte de médicament un code barre unique en deux dimensions, un Datamatrix, correspondant notamment à (1) un numéro de série unique, (2) le code produit du fabricant sous la forme d'un numéro d'article commercial global ou GTIN[49] (GS1), (3) un numéro de lot et (4) la date d'expiration du médicament ainsi qu'un dispositif anti-effraction sur l'emballage des médicaments soumis à prescription[50]. Meditect a testé, avec le laboratoire pharmaceutique UPSA, l'extension de la sérialisation européenne des médicaments à ceux destinés au marché africain. L'entreprise a également développé deux applications mobiles à destination des pharmaciens et des « patients/clients » en Afrique. A l'aide de *Meditect Pro*, le pharmacien du réseau scanne le Datamatrix sur la boîte de médicament pour en vérifier l'authenticité. L'application *Meditect Patient* permet à n'importe qui, équipé d'un smartphone ou d'un *feature phone** de vérifier que les médicaments ne sont pas falsifiés.

Le laboratoire pharmaceutique, client de Meditect, peut suivre, sur un tableau de bord en ligne, la distribution et la géolocalisation des ventes de ses médicaments. Le système a été testé sur les boîtes d'Efferalgan vendues en Côte d'Ivoire, soit environ un million de boîtes[51], et devrait prochainement être déployé au Cameroun et au Sénégal. D'un point de vue technique, la blockchain de Meditect est un *fork** du protocole Bitcoin Core, adapté au service d'échanges et de vérification de numéros sérialisés qui permet uniquement au laboratoire qui a produit le médicament et à Meditect d'ajouter des données à l'identifiant et qui permet à chaque partie prenante

49 *Global Trade Item Number*, Code article international : un code identifiant toute unité commerciale à l'international de manière unique.
50 « Médicaments falsifiés: une nouvelle réglementation pour une meilleure sécurité des patients », European Commission, 8 février 2019, https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_872
51 « Comment Meditect a peaufiné sa solution de traçabilité du médicament avec UPSA », Aurélie Dureuil, MindHealth, 16 mars 2021, https://www.mindhealth.fr/industrie/post-commercialisation/comment-meditect-a-peaufine-sa-solution-de-tracabilite-du-medicament-avec-upsa/



The pharmaceutical supply chain.
Source : « PharmaCrypt: Blockchain for Critical Pharmaceutical Industry to Counterfeit Drugs, », N. Saxena, I. Thomas, P. Gope, P. Burnap and N. Kumar, in *Computer*, vol. 53, no. 7, July 2020, pp. 29-44, doi: 10.1109/MC.2020.2989238

tout au long du cycle de vie (laboratoire, grossiste, distributeur, consommateur) d'accéder aux informations de la blockchain et de les vérifier à l'aide d'une application[52]. C'est une blockchain privée avec permission dont le code source est public[53].

Aux Etats-Unis, le projet **Mediledger** se présente comme une blockchain privée avec permission et rassemble une trentaine d'acteurs de la chaîne logistique. L'initiative a pour ambition d'utiliser un registre distribué pour se conformer aux exigences de sérialisation et d'interopérabilité du *Drug Supply Chain Security Act* (DGSCA), qui deviendront obligatoires aux Etats-Unis en novembre 2023[54].

Quant à **StaTwig,** une *startup* créée à Singapour et en Inde en 2016**,** elle développe **VaccineLedger**, « *une plateforme* open source *conçue pour assurer la traçabilité de bout en bout des vaccins au niveau des flacons dans la chaîne d'approvisionnement mondiale* ». La *startup*, financée en partie par le Fonds d'innovation de l'UNICEF a également été nommé « innovateur mondial » au sein du Forum économique mondial (WEF) en 2020[55].

52 « Meditect: Saving lives with the blockchain », Cristoffer Harlos, Medium, October 17, 2018, https://medium.datadriveninvestor.com/meditect-saving-lives-with-the-blockchain-3124b364ae4e
53 « Meditect », Github, retrieved May 16 2022, https://github.com/Meditect/blockchain_go /
54 « What You Need to Know about the Drug Supply Chain Security Act », Rob Besse, Pharmexec, March 18, 2020, https://www.pharmexec.com/view/what-you-need-know-about-drug-supply-chain-security-act
55 « UNICEF Innovation Fund Graduate: Statwig », Sid Chakravarthy, March 30, 2020, https://www.unicef.org/innovation/fundgraduate/StaTwig

Les informations enregistrées sur la plateforme concernent l'identification des vaccins sur la chaîne de production mais également d'autres informations critiques comme notamment la température et l'humidité afin de garantir que la chaîne de conservation est bien respectée et que les vaccins sont correctement conservés.

VaccineLedger, dont le code source est public[56] sous licence MIT, a été développé avec l'aide de LACChain[57], une alliance réunissant différents acteurs de l'écosystème blockchain en Amérique latine et dans les Caraïbes et dirigée par le Laboratoire d'innovation du Groupe de la Banque interaméricaine de développement (IDB Lab[58]).

56 « The Ledger », GitHub, retrieved May 16, 2022, https://github.com/statwig-com/theledger
57 « Caracteristicas de LACChain », LACCHain, retrieved May 16, 2022, https://www.lacchain.net/home ?lang=en
58 BID Lab, « About », https://bidlab.org/en/about

ENJEUX ET QUESTIONS

Alors que les scandales liés à l'exposition ou à la fuite de données de santé ne cessent de croître partout dans le monde[1], les blockchains et notamment la notion d'identité décentralisée (voir Chapitre Identité et propriété) apporte une réponse originale à la gestion et la sécurisation des données de santé.

En effet, **l'apparente contradiction des enjeux liés à ces données sensibles consiste tout à la fois à assurer, voire garantir, leur confidentialité tout en favorisant leur partage selon le contexte d'utilisation**. Une personne peut avoir besoin de partager un document de santé avec un employeur sans que ce dernier n'accède et conserve des informations personnelles.

L'European Blockchain Services Infrastructure (EBSI) a ainsi pour projet de lancer un « passeport européen de sécurité sociale » afin de mettre en œuvre la vérification transfrontalière de la couverture sociale des travailleurs détachés. Cela signifie « *qu'une institution compétente en matière de sécurité sociale dans un État membre délivre un document sous la forme d'une attestation vérifiable et qu'un inspecteur dans un autre État membre le vérifie*[2] *»*. Une personne peut également souhaiter partager ses données de santé à des fins de recherche médicale en ayant la garantie de ne pas pouvoir être retrouvé individuellement.

L'innovation dans les domaines de la médecine et de la recherche médicale dépend intrinsèquement de la quantité de données mise à la disposition des chercheurs. Ce qui revient également à se poser la question de la patrimonialité ou non des données personnelles de santé, avec deux visions différentes entre celle anglo-saxonne pour qui les données de santé peuvent faire l'objet de commerce, et celle européenne qui vise à considérer ces données comme sensibles.

Mis à part le domaine du séquençage génétique, où des *startups* proposent une architecture technique résolvant l'apparente contradiction entre la sécurisation des données des clients et leur partage à des fins de recherche scientifique,

1 List of data breaches > Healthcare https://en.wikipedia.org/wiki/List_of_data_breaches
2 Navigating the EBSI Use Cases Social security, EBSI, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Use+cases

force est de constater que la plupart des initiatives que nous avons identifiées reposent sur la mise en œuvre de blockchains privées, que ce soit dans les domaines de la gestion des données de patient, de la recherche de nouveaux médicaments ou encore des essais cliniques.

La question du rôle des États dans la mise en œuvre de systèmes d'identité décentralisés, afin notamment d'être utilisés dans le cadre d'une réforme globale des systèmes d'information manipulant des données de santé reste entière.

De plus, l'éventuelle appropriation des données de santé par les individus ne ferme pas la question de la marchandisation de ces dernières. En effet, un système dans lequel les individus sont propriétaires de leurs données de santé leur permettrait de les vendre à qui est le plus offrant. Si, en théorie, l'idée peut sembler séduisante, elle soulève toutefois des questions éthiques. Des citoyens vivant sous le seuil de pauvreté se verraient-ils contraints de donner un accès à leurs données de santé afin de bénéficier d'aides provenant de l'hémisphère nord ? En quoi des initiatives blockchain pourraient-elles apporter des éléments de réponse à cette problématique ?

Il s'avère en tout cas que les blocages sont actuellement plus politiques que techniques et que les enjeux financiers du marché de la santé dépassent encore largement les enjeux sociaux et éthiques tenant à la confidentialité des données de santé de tout un chacun.

GLOSSAIRE

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

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

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

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

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

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

Block Explorer : Voir “explorateur blockchain”.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Wallet - Portefeuille : voir "portefeuille d'identité"

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

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