



# EDUCATION & EMPLOI

SEPTEMBRE 2022

[WWW.BLOCKCHAINFORGOOD.FR](http://WWW.BLOCKCHAINFORGOOD.FR)



BLOCKCHAIN  
@POLYTECHNIQUE

**bpifrance**  
SERVIR L'AVENIR



INSTITUT  
Louis Bachelier

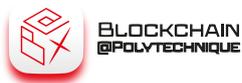
**PB** PositiveBlockchain.io

## 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 ÉDUCATION & EMPLOI

[Noémie Dié](#), [Christophe Gbossou](#), [Alejandro Gómez](#), [Audran Gouis](#).

# TABLE DES MATIÈRES

ÉDUCATION ET DIPLÔMES -----	7
MARCHÉ DU TRAVAIL -----	13
ENCADRÉ : LE FINANCEMENT QUADRATIQUE -----	16
DROITS DES TRAVAILLEURS -----	18
ENJEUX ET QUESTIONS -----	22
GLOSSAIRE -----	24
ÉDITEUR -----	34

## ÉDUCATION ET EMPLOI

Nombre de projets dans la base : 38

Nombre de projets actifs : 20

**Nom des projets actifs** : African Blockchain Center for Developers ; AmwFund ; APPII ; BCDiploma ; BitDegree ; Blockcerts ; Code to inspire ; Credly ; DirectEd - Direct donation for education ; Diwala ; eMin ; Indorse ; Misthos ; Odem.io ; Open Badges ; Opolis ; Proof of Learn ; Prosoon ; Steam Role ; UNICEF Giga ; *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](mailto: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 Objectifs de développement durable 4 et 8 visent notamment à assurer l'accès de tous à une éducation équitable, inclusive et de qualité, la possibilité d'apprentissage tout au long de la vie, ainsi qu'un plein emploi et un travail décent pour tous. Nous avons identifié une vingtaine d'initiatives blockchain qui concourent à ces Objectifs, dans les domaines de l'éducation et de la certification de diplômes, des Organisations autonomes décentralisées\* sur le marché du travail ou encore de la transparence des conditions de travail de populations fragiles.**

Que ce soit pour certifier un diplôme, une formation, une expérience, un contrat de travail, ces initiatives blockchain s'appuient nécessairement sur l'identité de la personne qui utilise ces services et invoque les notions d'identité décentralisée et d'attestations vérifiables à propos desquelles nous avons

consacré un chapitre entier sur le sujet au chapitre Identité & propriété. L'apport des blockchains dans le domaine de l'identité numérique est d'inverser le modèle actuel fondé sur l'authentification et le contrôle d'accès d'une personne, géré tout deux par une organisation, vers un modèle fondé sur la vérifiabilité d'attestations contrôlées par cette même personne.

### Education et diplômes

Le cas d'usage le plus répandu dans le domaine de l'éducation est celui de la certification de diplômes où l'usage de blockchain permet de maintenir l'intégrité d'un registre sans qu'il ne soit plus centralisé. Il est à la fois extrêmement difficile de falsifier un tel registre et très simple pour une entreprise de vérifier dans ce même registre si un candidat est bel et bien diplômé de ladite école. **APPII** en Angleterre, **Smart Certificate** en Belgique, **Diwala** en Norvège,



**Blockademia** en Croatie, **BCDiploma** ou **Prosoon** en France sont quelques-unes de ces entreprises et *startups* déployant ce service de certification de diplôme. Dès 2016, des projets pilotes ont été menés au Kenya ou encore en Inde, en 2018, où cinq millions d'étudiants sont diplômés chaque année<sup>1</sup>. Comme l'explique **Odem**, une plateforme décentralisée créée en 2017 à Zug en Suisse qui relie sans intermédiaire les employeurs, les étudiants et les formateurs, « *la façon dont nous apprenons, travaillons, recrutons et formons a évolué de façon spectaculaire ces dernières années mais l'infrastructure sous-jacente qui soutient cet écosystème n'a pas changé* ».

Régulièrement dénoncée par les écoles et par les entreprises, la fraude au diplôme serait un fléau en constante progression. Au point que des entreprises, comme Verifdiploma fondée en France en 2001, se sont lancées sur ce seul créneau d'authentification des diplômes et des expériences professionnelles de candidats. La France compte quelque 3 500 établissements d'enseignement supérieur, parmi lesquels 500 établissements publics (universités, écoles d'ingénieurs, écoles de commerce, écoles d'art et écoles d'architecture) et

quelque 3 000 écoles et instituts privés<sup>2</sup>. Chaque année, Verifdiploma reçoit de la part de 2 500 d'entre eux la liste des nouveaux diplômés que l'entreprise conserve au sein d'une base de données centralisée, et se targue de passer au crible quelque 115 000 CV par an<sup>3</sup>.

La promesse d'initiatives blockchain dans le domaine de la vérification de diplômes consiste à offrir tout à la fois aux établissements supérieurs et aux candidats un moyen, sécurisé, de prouver aux employeurs la véracité de leurs diplômes, sans que le service ne passe plus par un quelconque intermédiaire. L'intérêt de la mise en place d'une telle infrastructure est double.

Pour les apprenants, elle permet de conserver un historique de leur apprentissage tout au long de la vie, et le partager, de manière sélective avec un employeur, sans avoir à solliciter ou payer un établissement pour obtenir une nouvelle copie d'un diplôme. Pour les établissements, elle permet de maintenir un registre de diplômes de manière sûre et peu coûteuse et ainsi considérablement réduire le risque de fraude, tout en soulageant les administrations sollicitées pour le renvoi de diplôme égaré.

1 « Blockchains and Education », Allan Third, Kevin Quick, Chris Valentine, Michelle Bachler, John Domingue, Knowledge Media Institute of the Open University, Knowledge Media Institute of the Open University for the European Union Blockchain Observatory and Forum, Dec 5 2019, [https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchain\\_observatory\\_education.pdf](https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchain_observatory_education.pdf)

2 « L'enseignement supérieur en France », EuroGuidance, retrieved May 31, 2022, <https://www.euroguidance-france.org/coming-venir-france/venir-en-france/lenseignement-superieur-france>

3 « Pour trouver un emploi, ils mentent sur leur diplôme », Chloé Marriault, start.Les Echos, 7 mai 2021, <https://start.lesechos.fr/travailler-mieux/recrutements-entretiens/pour-trouver-un-emploi-ils-mentent-sur-leur-diplome-1313415>

De telles initiatives ont émergé un peu partout dans le monde, en Europe, aux États-Unis, en Inde ou encore en Afrique. En Italie, **Almacert**, conçu par FlossLab<sup>4</sup> en 2018 et développé en collaboration avec l'Université de Cagliari, « offre aux universités européennes la possibilité de certifier les suppléments au diplôme de leurs diplômés grâce à la blockchain publique Ethereum ».

Le **Digital Credential Consortium**, créé en 2018 par douze universités aux États-Unis, en Allemagne, au Canada, au Mexique et en Italie<sup>5</sup>, et hébergé au Massachusetts Institute of Technology, a pour vocation de déployer « une infrastructure de confiance, distribuée et partagée qui devient la norme pour l'émission, le stockage, la présentation et la vérification de titres universitaires numériques<sup>6</sup> ».

Annoncé en mai 2021, en France, **l'Université de Lille** délivre dorénavant à ses étudiants un diplôme ainsi qu'une attestation numérique<sup>7</sup>. 20 000 étudiants diplômés en 2020 ont reçu

*« un lien pérenne vers un document web infalsifiable et vérifiable, traduit en anglais, qu'il ou elle pourra présenter à un employeur, une association ou en poursuite d'études, en France et à l'étranger, permettant de vérifier l'authenticité du diplôme<sup>8</sup> ».*

En avril 2021, le **gouvernement éthiopien** a signé un accord pour mettre en place une solution d'identité numérique décentralisée auprès des cinq millions d'étudiants répartis dans les 3 500 écoles du pays<sup>9</sup> afin notamment de leur permettre de bénéficier d'attestations numériques certifiant leur diplôme (Voir chapitre Identité & Propriété).

Obtenir une copie de son diplôme dans des pays dont le système d'éducation est mature ne pose pas de problème majeur. Il en est autrement dans les pays dont le système d'éducation est défaillant.

Le ministère éthiopien de l'éducation ne dispose aujourd'hui d'aucune donnée ni d'aucune visibilité sur les résultats scolaires avant la dernière année

4 « Metafora », Flosslab, retrieved May 31, 2022, <https://www.flosslab.com/>

5 Delft University of Technology (The Netherlands) Georgia Tech (USA) Harvard University (USA) Hasso Plattner Institute, University of Potsdam (Germany) Massachusetts Institute of Technology (USA) McMaster University (Canada) Tecnológico De Monterrey (Mexico) TU Munich (Germany) UC Berkeley (USA) UC Irvine (USA) University of Milano-Bicocca (Italy) University of Toronto (Canada).

6 « Our Technology », Digital Credentials Consortium, retrieved May 31, 2022, <https://digitalcredentials.mit.edu/>

7 « Des attestations numériques pour tous les diplômé·e·s de l'Université de Lille », Université de Lille, Communiqué de Presse, 28 mai 2021, [https://www.univ-lille.fr/fileadmin/user\\_upload/presse/presse\\_2021/CPDemattestoklien.pdf](https://www.univ-lille.fr/fileadmin/user_upload/presse/presse_2021/CPDemattestoklien.pdf)

8 « 20 000 attestations numériques de réussite au diplôme émises par l'Université de Lille », Université de Lille, Communiqué de Presse, 10 février 2022, [https://newsroom.univ-lille.fr/fileadmin/user\\_upload/presse/2022/v20.000attestationsnumeriques.pdf](https://newsroom.univ-lille.fr/fileadmin/user_upload/presse/2022/v20.000attestationsnumeriques.pdf)

9 « Ethiopia's blockchain deal is a watershed moment for the technology, and for Africa », Iwa Salami, The Conversation, 20 mai 2021, <https://theconversation.com/ethiopias-blockchain-deal-is-a-watershed-moment-for-the-technology-and-for-africa-160719>



d'école, lorsque les élèves quittent le système éducatif. En tenant un registre infalsifiable sur la blockchain publique **Cardano** et en utilisant le système d'identité décentralisé **Atala Prism**, le pays compte résoudre le fait « *qu'il est pratiquement impossible pour les étudiants de prouver leurs résultats scolaires à des employeurs potentiels ou à des établissements d'enseignement supérieur, ce qui limitait souvent considérablement leurs perspectives* »<sup>10</sup>.

**Diwala**, créé entre la Norvège et l'Ouganda en 2018 est une plateforme qui permet « *l'émission et la vérification sécurisées et efficaces de certificats ou de titres de compétences et s'efforce de servir la population de 1,8 milliard de personnes dans le monde qui vivent sans identité numérique et qui sont incapables de prouver leur éducation, leur travail et leur historique financier* ».

Diwala, est parti du constat que la fraude aux certificats est un problème majeur pour le système d'éducation en Ouganda. L'entreprise explique que « *lorsqu'un étudiant obtient son diplôme dans une université ougandaise, il reçoit une copie papier (le document officiel avec le sceau) et une copie électronique*

*de son diplôme (un papier qui tient lieu de document réel). Afin de valider leur diplôme, les étudiants doivent ensuite obtenir différents tampons et signatures de diverses sources. Malheureusement, ces processus peuvent prendre beaucoup de temps ; des étudiants ont rapporté qu'il leur a fallu jusqu'à six mois pour recevoir leur certificat après l'obtention de leur diplôme. Les processus de validation nécessaires pour vérifier les certificats peuvent coûter jusqu'à 2 ou 300 dollars, en fonction du nombre de certificats que vous possédez* ».

La plateforme s'appuie sur **uPort**, scindé depuis 2021 en deux projets, **Serto**, une solution logicielle « low code<sup>11</sup> » d'identité décentralisée et **Veramo**, un *framework* JavaScript qui permet à quiconque « *d'utiliser facilement des données cryptographiquement vérifiables dans ses applications, et de mettre en œuvre des DID<sup>12</sup>, des attestations vérifiables et des protocoles centrés sur les données pour offrir des fonctionnalités de nouvelle génération à leurs utilisateurs<sup>13</sup>* ».

Depuis 2016, **deux méthodes pour garantir l'authenticité d'un diplôme ont été expérimentées**. Celle consistant à horodater et inscrire un diplôme dans

10 « Atala Prism » Project Management Institute, retrieved May 31, 2022, <https://www.pmi.org/most-influential-projects-2021/50-most-influential-projects-2021/atala-prism>

11 No code / low code : « Nouvelle tendance dans le secteur de l'informatique liée à l'apparition de plateformes de développement sans code, en anglais « No code development platform » (NCDPs). Ces structures offrent la possibilité à des personnes sans aucune compétence technique de créer toutes sortes d'applications web par le biais d'interfaces graphiques et de panneaux de configurations, sans passer par une programmation informatique traditionnelle»,. Source : « No code », Jacques-André Fines-Schlumberger, *La revue européenne des médias et du numérique*, N°54bis-55 Automne 2020 <https://la-rem.eu/2020/12/no-code/>

12 Voir « Chapitre Identité et propriété »: Identité décentralisée - DID

13 « Introduction », Veramo, retrieved May 31, 2022, <https://veramo.io/docs/basics/introduction>

une blockchain, comme les initiatives menées par l'école d'ingénieurs Holberton à San Francisco, aux États-Unis, avec la société **Bitproof**<sup>14</sup>, par l'École Supérieure d'Ingénieurs Léonard-de-Vinci (ESILV) en 2016, ou encore par l'École nationale supérieure Mines-Télécom Atlantique Bretagne (IMT Atlantique) en 2017, en partenariat avec la *startup* **Woleet**, spécialisée dans l'ancrage de documents dans une blockchain<sup>15</sup> et Digiposte, la solution de coffres forts numériques du groupe La Poste. « *Chaque diplômé a reçu, en plus de son diplôme papier, une version numérisée de celui-ci accompagnée d'un certificat d'ancrage dans la blockchain de Bitcoin*<sup>16</sup> » expliquait Marianne Laurent, alors chargée de mission innovation et créativité à l'IMT Atlantique.

Une autre méthode consiste à s'appuyer sur un système d'identité décentralisé / attestations vérifiables<sup>17</sup>, à l'instar de **Prosoon** qui permet d'émettre des attestations vérifiables sur plusieurs infrastructures compatibles Ethereum Virtual Machine (EVM\*), comme Ethereum, Tezos, Polygon ou encore Solana.

Selon le **Digital Credential Consortium**, « *une attestation vérifiable peut être imaginée comme la combinaison de deux*

*éléments : un document et une enveloppe dans laquelle ce document est placé. Le document est comme le morceau de papier qu'une université délivre à un diplômé, qui contient le nom du destinataire ainsi qu'une description du titre qu'il a reçu. L'enveloppe protège le contenu du document afin qu'il ne puisse pas être modifié et qu'il communique de manière fiable l'authenticité de son contenu*<sup>18</sup> ».

S'appuyer sur un écosystème d'identité décentralisée et d'attestations d'éducation vérifiables\* semble être une aubaine pour l'ensemble des acteurs interagissant entre eux : les apprenants, qu'il s'agisse de leur premier diplôme ou d'une formation effectuée ultérieurement, les établissements de formation et les employeurs ou tout tiers susceptibles de vérifier l'authenticité d'un diplôme.

Pour un apprenant, il s'agit de détenir, en propre, des attestations vérifiables correspondant à l'ensemble de ses diplômes et formations tout au long de la vie, y compris si l'établissement ferme. Et de pouvoir les partager, de manière sélective ou non, avec un tiers (employeurs, services publics, organisations professionnelles etc.) en ayant l'assurance que ces informations ne seront pas exploitées à son insu.

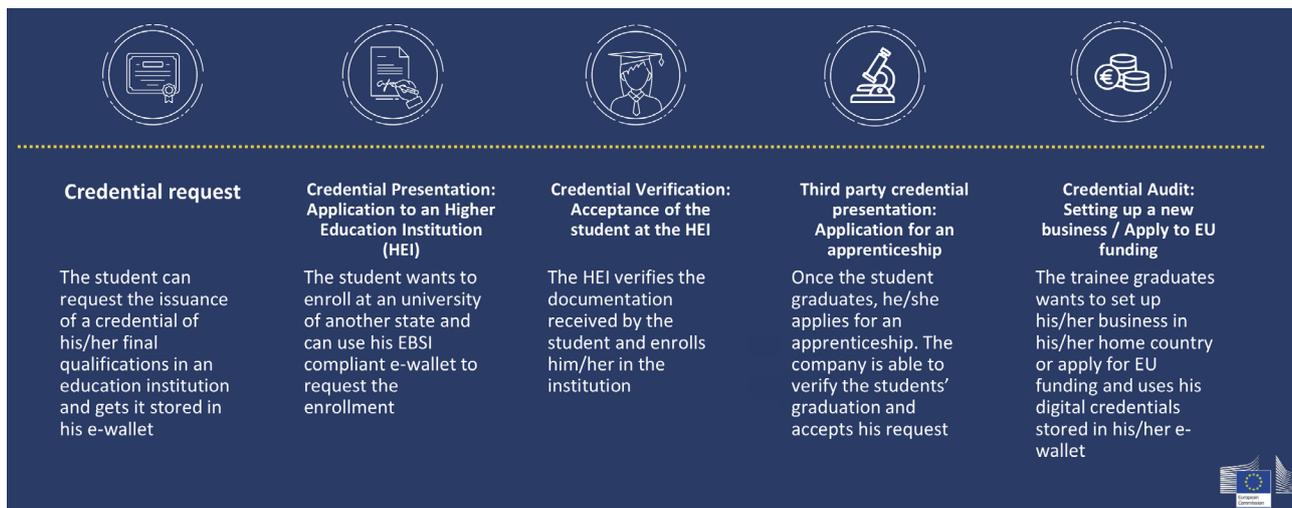
14 « Les blockchains et le droit », Boris Barraud, Revue Lamy Droit de l'immatériel, Lamy (imprimé) / Wolters Kluwer édition électronique 2018, pp.48-62.fhal-01729646f

15 Voir « Chapitre Identité et propriété ».

16 « Votre diplôme dans la blockchain, quels avantages ? », Marianne Laurent, Monde des Grandes Ecoles et Universités, 16 mai 2017, <https://www.mondedesgrandesecoles.fr/diplome-blockchain-avantages/>

17 Voir « Chapitre Identité et propriété ».

18 White paper: « Building the digital credential infrastructure for the future », February 2020, <https://digitalcredentials.mit.edu>



### EBSI Use case: *Diplomas management. Overview of core functionalities.*

Source : « European Blockchain Service Infrastructure », Daniel Du Seuil – ESSIF convenor and Belgian representative in EBP, OECD, Interreg, <https://northsearegion.eu/media/16680/ebsi-explained-by-daniel-du-seuil.pdf>

Pour un établissement de formation, le premier intérêt est de s'appuyer sur des standards qui garantissent l'intégrité et la confidentialité des informations des apprenants tout en étant bien moins coûteux à mettre en œuvre qu'un système centralisé ou externalisé.

C'est également un gain de temps pour les équipes administratives chargées d'envoyer la copie de diplômes égarés par les apprenants. Pour l'employeur enfin, c'est la garantie de recevoir des CV dont les diplômes sont certifiés sans recourir à un tiers pour en vérifier l'authenticité et pour un coût proche de zéro. Sur le marché du recrutement, cela permet également de favoriser l'usage du CV anonyme qui consiste à respecter l'égalité des chances et lutter contre les discriminations à l'embauche dans

un processus de recrutement portant uniquement sur les compétences et les diplômes d'un candidat sans accéder à son identité et son nom, tant qu'il n'est pas sollicité pour un entretien<sup>19</sup>.

Face à la diversité de ces initiatives, l'intérêt de s'appuyer sur un système d'attestations vérifiables permettrait d'assurer une interopérabilité des différents services de certification de diplômes en utilisant des standards communs.

C'est l'objet de l'Infrastructure Européenne de Service Blockchain (*European Blockchain Services Infrastructure - EBSI*<sup>20</sup>) dont nous parlons au Chapitre « Gouvernement et démocratie ». L'EBSI est une initiative conjointe de la Commission européenne

<sup>19</sup> « Discriminations à l'embauche : un phénomène qui reste "généralisé et persistant" », Louise Couvelaire, 24 novembre 2021/ [https://www.lemonde.fr/societe/article/2021/11/24/discriminations-a-l-embauche-un-phenomene-qui-reste-generalise-et-persistant\\_6103458\\_3224.html](https://www.lemonde.fr/societe/article/2021/11/24/discriminations-a-l-embauche-un-phenomene-qui-reste-generalise-et-persistant_6103458_3224.html)

<sup>20</sup> « Introducing EBSI », European Commission, retrieved May 31 2022, <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/>

et de l'*European Blockchain Partnership* dont l'objet est de s'appuyer sur la standardisation de blockchains pour « *accélérer la création de services transfrontaliers pour les administrations publiques et leurs écosystèmes afin de vérifier les informations et de rendre les services plus fiables*<sup>21</sup> ». Depuis 2020, EBSI déploie un réseau de nœuds distribués à travers l'Europe, soutenant des applications axées sur des plusieurs cas d'usage dont notamment celui de la certification des diplômes<sup>22</sup> :

Ce qui s'inscrit dans ses efforts, entamés avec le Conseil de l'Europe et de l'UNESCO/CEPES depuis 1996, d'améliorer la transparence internationale et de faciliter la reconnaissance académique et professionnelle des qualifications telles que les diplômes, les acquis universitaires, les certificats et la formation en général.

De plus, un diplôme n'est bien souvent que le reflet d'un enseignement commun sans qu'il ne soit possible de revendiquer la granularité de ses composantes, comme les modules, les cours, les stages, les dissertations, les cas pratiques etc. Sur le modèle européen des ECTS Système Européen de transfert d'unités de cours capitalisables (European Credit Transfer System - ECTS), mis en place en 1989 dans le cadre du programme

Erasmus pour faciliter la reconnaissance académique des périodes d'études réalisées à l'étranger, et de développer qualitativement la mobilité des étudiants en Europe, il pourrait être imaginé de certifier non plus seulement un diplôme mais des « des unités de cours ».

La certification de diplômes et des apprentissages n'est probablement qu'une première étape vers la certification, plus globale, de parcours et d'expériences professionnels, tout au long de la vie des individus, de plus en plus mobiles, en adéquation avec un marché du travail en pleine mutation.

### Marché du travail

Il est imaginable de transposer la certification de diplômes à la certification d'expériences professionnelles.

L'émetteur d'une attestation vérifiable ne serait plus un établissement d'enseignement mais une entreprise, certifiant qu'une personne a bien travaillé en son sein.

Par exemple, **Talent Cloud**<sup>23</sup>, dirigé par Valérie Thomas, responsable de la stratégie de mobilité des talents pour le Secrétariat du Conseil du Trésor du Canada, est une initiative qui développe de nouveaux modèles de recrutement et

21 « What is EBSI ? », European Commission, retrieved May 31, 2022, <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi>

22 « Diploma Functional Scope Skip to end of metadata », Marta Pastor, Regina dela Eva, European Commission, May 26, 2021, <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Diploma+Functional+Scope>

23 « Talent Cloud Results Report », Government of Canada, retrieved May 31 2022, <https://talent.canada.ca/en/2000/01/01/504-blockchain.html>



de mobilisation des talents dans le secteur de la fonction publique au Canada. L'idée de Talent Cloud est d'offrir aux salariés et employeurs plus d'information qu'un simple diplôme, comme « *des descriptions fondées sur les compétences qui peuvent être mises en correspondance de manière plus précise avec les aptitudes/compétences*<sup>24</sup> », explique Kim Hamilton Duffy, du Digital Credentials Consortium (voir *supra*). Hugo Spiess, fondateur de Prosoon, explique ainsi que « *les micro certifications permettent de valoriser les compétences et les expériences des apprenants au-delà des diplômes, permettant aux recruteurs une analyse plus précise sur les qualifications et les centres d'intérêts des candidats*<sup>25</sup> ».

Certaines entreprises s'intéressent à la manière dont les blockchains et les crypto-actifs pourraient impacter la gestion de la paie au sein des entreprises, notamment afin d'automatiser et sécuriser le paiement de salaire transfrontalier. ADP Inc., un fournisseur américain de solutions d'externalisation professionnelles relatives à la gestion du capital humain (paie, temps et activités et ressources humaines) et qui emploie quelque 60 000 collaborateurs dans le monde, explore ces potentialités depuis 2018 et a même déposé un brevet en 2019 sur une

« Payroll Based Blockchain Identity<sup>26</sup> » qui repose sur la blockchain **Ripple**, une blockchain publique permissionnée gérée par des intermédiaires bancaires et financiers<sup>27</sup>.

Le projet d'innovation **Impact** du Programme alimentaire mondial (PAM) relie des étudiants non bancarisés, menacés par la faim, à l'économie numérique mondiale par le biais d'une plateforme de micro-travail et d'un portefeuille de crypto-actifs. Partant du constat que l'industrie de l'annotation des données (*data annotation industry*) dans le domaine de l'intelligence artificielle (IA) est en plein essor, le Programme alimentaire mondial a construit, avec Corsali et **Celo**, le programme EMPACT *digital training*, à destination des travailleurs du secteur informel de pays en développement, en s'adressant tout particulièrement à ceux qui n'ont pas accès aux institutions financières et ne disposent pas de comptes bancaires pour recevoir des paiements.

Le projet a débuté en 2016 et six ans plus tard, 13 500 jeunes réfugiés et jeunes défavorisés, dont 54 % de femmes, en Colombie, en Irak, au Kenya, au Liban, en Palestine, en Turquie et au Zimbabwe ont pu en bénéficier.

24 « Blockchain Can Disrupt Higher Education Today, Global Labor Market Tomorrow », Andrew Singer, The CoinTelegraph, June 14, 2020, <https://cointelegraph.com/news/blockchain-can-disrupt-higher-education-today-global-labor-market-tomorrow>

25 Entretien avec Hugo Spiess, fondateur de Prosoon, Association Blockchain for Good, 30 juin 2022.

26 « Payroll based blockchain identity », United States Patent Application, FPO, November 8, 2018, <https://www.freepatentsonline.com/y2018/0322587.html>

27 Ripple permet aux institutions financières qui font partie du réseau RippleNet d'envoyer et recevoir de l'argent dans le monde entier instantanément et pour des frais de transactions modiques. Ripple : <https://ripple.com/faq/>

Ian Kimaru, 27 ans, habitant le plus grand bidonville du Kenya à Kibera témoigne ainsi : « *en trois mois seulement, je me suis familiarisé avec de nouveaux outils informatiques et j'ai appris le codage et le développement web grâce à un cours sur mesure sur la plateforme d'apprentissage Pluralsight*<sup>28</sup>. *Ces nouvelles compétences m'ont ouvert d'énormes possibilités sur le marché mondial de l'emploi dans le secteur numérique, puisque je pouvais proposer des emplois informatiques en freelance sur l'internet*<sup>29</sup> ».

Corsali est une plateforme d'apprentissage automatique alimentée par des travailleurs indépendants étiquetant des données contre rémunération depuis leurs téléphones portables<sup>30</sup>. La plateforme de micro-travail intègre un portefeuille de crypto-actifs, permettant aux participants d'être payés instantanément en dollars Celo (cUSD), une crypto-actif stable\* indexé au dollar américain, qu'ils peuvent en outre convertir en monnaie locale avec l'application populaire MPESA, suivant le pays dans lequel il se trouve.

Ce type d'initiative menée par le Programme alimentaire mondial (PAM) ne pourrait pas passer par une banque ou un intermédiaire financier dont les frais empêchent tout micropaiement.

Pour d'autres, l'avenir du marché du travail réside dans les Organisations autonomes décentralisées (DAO\*). Il s'agirait, pour certains, de passer d'un contrat de travail à plein temps pour un seul employeur à des contributions périodiques pour plusieurs organisations autonomes, la gestion des contrats, des missions, des paiements et même des cotisations étant prises en charge automatiquement par ce nouveau type de structure.

Pour Steve Glaveski auteur de « *Time Rich : Do Your Best Work, Live Your Best Life* », « *au lieu de travailler depuis un bureau central toute l'année et d'avoir deux à quatre semaines de congé, la plupart des contributeurs de DAO travailleront probablement à distance, se lieront dans des espaces sociaux virtuels tels que **CryptoVoxels** ou **The Sandbox**, et pendant plusieurs jours ou semaines par an, se réuniront dans la vraie vie pour des conférences et des retraites inspirantes*<sup>31</sup>. Cette vision du marché du travail de demain ne va pas nécessairement dans le sens d'un appauvrissement de travailleurs indépendants, notamment ceux de l'économie des petits boulots (*Gig economy*).

Une initiative menée par **Gitcoin** donne à voir un aperçu de la manière dont une communauté de travail, ici informatique,

28 « Our latest picture », PluralSight, retrieved May 31 2022, <https://www.pluralsight.com/>

29 « Tech Training Tackles Youth Unemployment in Kenya's Largest Urban Slum — Five Personal Stories from Kibera », WFP Innovation Accelerator, Oct 30 2020, <https://wfpinnovation.medium.com/tech-training-tackles-youth-unemployment-in-kenyas-largest-urban-slum-five-personal-stories-6b636e0b741c>

30 « Corsali — Founders Series », Amy Slawson, Medium, Jun 22 2021, <https://medium.com/virtuous-ventures/corsali-founders-series-991dd20436ee>

31 « How DAOs Could Change the Way We Work », Steve Glaveski, Harvard Business Review, Apr 07 2022, <https://hbr.org/2022/04/how-daos-could-change-the-way-we-work>



peut interagir à travers une Organisation autonome décentralisée (DAO\*). Gitcoin se présente comme « *une plateforme où vous êtes payés pour travailler sur des logiciels open source* » parmi lesquels des langages de programmation, de développement, des langages web ou encore de *design*.

Plus exactement, GitcoinDAO réunit un marché à deux versants avec d'un côté, des développeurs informatiques et de l'autre, des personnes ou des entreprises qui financent le développement de logiciels *open source*.

GitcoinDAO se présente ainsi comme « *une communauté de citoyens de l'Internet qui construit et finance des biens publics numériques, comme les logiciels libres*<sup>32</sup> ».

Lancée de Boulder aux Etats-Unis en 2017, Gitcoin a levé 62 millions de dollars, permettant de financer le travail de plus de 310 000 développeurs informatiques dans le monde à travers 2 400 projets. Pour ses utilisateurs, la mise en œuvre d'une DAO\* permet d'éviter la bureaucratie, se passer de tiers de confiance, d'éviter les frais liés au paiement internationaux et aux cartes de crédit en se reposant sur le token de Gitcoin.

Gitcoin<sup>33</sup> est construit sur la blockchain publique sans permission Ethereum et remplit deux fonctions. La première est de procéder au financement de

logiciels *open source*, levant des fonds en crypto-actifs à travers un système de financement participatif (*crowdfunding*) quadratique.

### Le Financement quadratique

Le financement quadratique est un système de financement s'inspirant des principes fondateurs du vote éponyme

#### Qu'est-ce que le vote quadratique ?

Le vote quadratique, ou système de vote à préférences multiples ordonnées, est un système de vote dans lequel les citoyens expriment leurs préférences à travers un crédit de voix dont ils disposent au départ. Chaque citoyen alloue ses crédits aux candidats qu'il souhaite. Les crédits représentent le « prix » qu'un électeur va devoir payer pour donner une voix à un candidat.

Cependant, le « prix » d'une voix n'est pas fixe : **chaque voix supplémentaire** donnée à un candidat **coûtera davantage de crédits** à l'électeur. Le « prix » en crédit correspond à la racine carrée du nombre de voix qu'il représente : 1 voix = 1 crédit, 2 voix = 4 crédits, 3 voix = 9 crédits, 4 voix = 16 crédits, 5 voix = 25 crédits, ... On dit alors que le « prix » en crédit évolue de manière quadratique.

#### Et au niveau du financement ?

Le financement quadratique s'est inspiré du système de vote éponyme pour lutter

32 « TLDR - What is Gitcoin ? [Updated May 2022] », Gitcoin, retrieved May 31 2022, <https://gov.gitcoin.co/tldr-what-is-gitcoin-updated-may-2022/8694>

33 « Gitcoin Core », Github, retrieved May 31, 2022, <https://github.com/gitcoinco>

contre la concentration du pouvoir de quelques gros investisseurs dans le financement des projets. Le système de financement quadratique comprend deux phases.

La première correspond à une allocation spontanée de l'argent des investisseurs vers les projets qui les intéressent. Certains projets récoltent plus ou moins d'argent, de la part d'un nombre plus ou moins important d'investisseurs. Seulement, le financement quadratique fait intervenir dans un second temps un mécanisme d'attribution des fonds d'une autre nature.

Le principe-clé en est le suivant : c'est **le nombre de contributeurs**, et non pas la somme initiale récoltée, qui **doit déterminer quel projet doit recevoir le plus**. Autrement dit, un projet ayant reçu des dons d'un nombre important de contributeurs se verra attribuer une somme d'argent plus importante que celle qu'il a récolté au départ. A contrario, un projet ayant reçu beaucoup d'argent de la part d'un petit nombre de contributeurs, verra finalement son financement diminuer.

Prenons l'exemple de deux projets ayant reçu initialement 100 GTC, la crypto-actif de Gitcoin. Le premier projet a reçu 100 GTC de la part d'un **seul donateur**, le second projet a aussi reçu 100 GTC de la part de **dix donateurs**. Grâce au financement quadratique, le projet 2 recevra finalement **190 GTC**, quand le projet 1 recevra seulement **10 GTC**.

La seconde fonction de la Gitcoin est la mise en relation de développeurs avec des porteurs de projets *open source*, la rencontre de l'offre et de la demande organisée autour d'une rémunération en crypto-actif pour le développeur. Par ces deux fonctions, Gitcoin préfigure l'une des facettes de l'économie de demain : d'une part, un financement plus horizontal de l'économie, évitant toute forme de concentration du capital investi dans un petit nombre de projets grâce au système quadratique ; et d'autre part, un marché du travail organisé en pair-à-pair, où l'offre et la demande de travail se rencontrent sans intermédiaire.



## Droits des travailleurs

### Organisations autonomes

**Misthos** ou encore **Opolis** font partie d'un mouvement, dans l'univers des crypto-actifs, visant à créer des modèles d'emploi moins centralisés qu'une entreprise traditionnelle, par le biais d'Organisations autonomes décentralisées\* ou encore de portefeuilles multi-signatures\*.

Créé en 2017 à Denver aux Etats-Unis, **Opolis** a d'abord été une coopérative numérique d'emploi (*Digital Employment Cooperative* - DEC) à destination des travailleurs indépendants pour leur permettre notamment de financer des prestations de santé, bénéficier de services partagés et utiliser un système de paiement inhérent à l'organisation autonome. En 2019, Opolis a reçu une subvention de développement de la part de la Fondation **MakerDAO**<sup>34</sup> afin d'intégrer sa crypto-actif DAI, un crypto-actif stable\*, au sein de la DAO\* Opolis. Aux Etats-Unis, les utilisateurs de la coopérative en ligne peuvent utiliser le crypto-actif stable\* Dai pour financer

leur adhésion, cotiser à une assurance maladie, cotiser à des plans de retraite et automatiser la conformité fiscale. Ils pourront choisir d'être payés en DAI ou en monnaie fiat. Opolis, en 2021, est devenue une « *réponse basée sur la blockchain à l'essor de la gig-economy*<sup>35</sup> », main-d'œuvre payée à la tâche et gérée *via* des applications mobiles proposées par des plateformes numériques (Uber, Deliveroo etc.) et une organisation professionnelle de l'emploi (*professional employment organization* - PEO) avec pour objectif de notamment faciliter les paiements transfrontaliers avec le crypto-actif stable\* DAI.

Le fondateur de **Misthos**, Justin Carter décrit ce modèle comme « *l'abandon d'une relation employé-employeur au profit d'un consensus de groupe sur l'apport de valeur*<sup>36</sup> ». Misthos, lancé à Berlin en Allemagne en 2017 est « *une application décentralisée de gestion collaborative des finances* ». C'est un portefeuille multi-signatures développé sur la plateforme d'applications décentralisées\* **Blockstack**<sup>37</sup>. Ce portefeuille est conçu pour que

34 « Decentralized Employment Ecosystem Opolis to Integrate MakerDAO's Dai Cryptocurrency », Danny Nelson, CoinDesk, September 18, 2019, <https://www.coindesk.com/markets/2019/09/18/decentralized-employment-ecosystem-opolis-to-integrate-makerdaos-dai-cryptocurrency/>

35 « Better work in the gig economy », Jacques-André Fines Schlumberger, *La Revue Européenne des Médias*, N°53 Hiver 2019-2020, <https://la-rem.eu/2020/03/better-work-in-the-gig-economy/>

36 « Blockstack's First Business App Wants to Help Employees Earn More Crypto », Leigh Cuen, CoinDesk, July 30, 2018, <https://www.coindesk.com/markets/2018/07/30/blockstacks-first-business-app-wants-to-help-employees-earn-more-crypto/>

37 Blockstack est une « *plateforme de développement d'applications décentralisées fonctionnant sur la blockchain Bitcoin. Elle apporte une solution à la décentralisation de l'authentification, de l'autorisation et du stockage des données sécurisées par la blockchain bitcoin. Avec Blockstack, les utilisateurs contrôlent leurs données et les applications s'exécutent sur leurs appareils. Il n'y a pas d'intermédiaires, pas de mots de passe, pas de silos de données massifs à violer et pas de services qui suivent les utilisateurs sur Internet* ». « Frequently Asked Questions », Misthos, retrieved May 31, 2022, <https://www.misthos.io/faq>

l'ensemble des participants d'un projet (équipe, financiers, autre organisations) puisse gérer la répartition des revenus, reçus sous forme de bitcoins, entre leurs membres.

Il est certain que ces services s'adressent aujourd'hui avant tout à un public spécialisé, travaillant pour la plupart dans l'écosystème des crypto-actifs. Opolis entretient d'ailleurs des liens étroits avec ConsenSys, le studio de conception d'Ethereum<sup>38</sup>. Mais ces expérimentations d'auto-organisation préfigurent peut-être les transformations futures de certaines organisations dont l'objectif est de mieux collaborer, notamment dans un environnement de travail à distance.

### Conditions de travail

En 2020, **VerifiK8**, une entreprise œuvrant à un développement durable et travaillant avec des entreprises agroalimentaires en Asie du Sud-Est, et Diginex Solutions, une entreprise technologique spécialisée dans les chaînes d'approvisionnement responsables, ont expérimenté **eMin**. eMin, développé par Diginex est un système basé sur la blockchain publique **Tezos** et dont l'objectif est de permettre au secteur privé d'identifier le travail forcé sur leurs chaînes d'approvisionnement. Et tout particulièrement les conditions de travail des ouvriers agricoles en

Thaïlande, secteur qui emploie plus de 11 millions de personnes et un nombre important de travailleurs migrants originaires du Myanmar, de la République démocratique populaire du Laos et du Cambodge.

Le projet pilote s'est adressé à deux groupes spécifiques d'ouvriers agricoles, en octobre et décembre 2020, afin de « *mieux comprendre leur risque d'exposition à l'esclavage moderne, leur intérêt pour le stockage sécurisé de leurs contrats et autres documents professionnels clés et leur niveau de confort avec la technologie*<sup>39</sup> » : Les travailleurs permanents ayant un contrat de travail officiel et les travailleurs saisonniers employés par le biais d'accords verbaux.

Si les premiers ont montré peu d'intérêt pour l'outil, les seconds se sont montrés plus sensibles à eMin. Ce second groupe, constitué de 58 travailleurs des secteurs de la canne à sucre, du riz et du caoutchouc dans le district de Nong Bua, Sikhorphum et Surin en Thaïlande, sont des villageois possédant de petites exploitations rizicoles à Nong Bua et deviennent des travailleurs agricoles saisonniers dans la province de Ratchaburi pendant la récolte de la canne à sucre.

38 « Blockstack's First Business App Wants to Help Employees Earn More Crypto », Leigh Cuen, CoinDesk, July 30, 2018, <https://www.coindesk.com/markets/2018/07/30/blockstacks-first-business-app-wants-to-help-employees-earn-more-crypto/>

39 « Using Frontier Technology to Detect Hidden Labour Abuses in Agricultural Sectors in Thailand », Leanne Melnyk, Juliette Alemany, Delta 8.7, Feb 26 2021, <https://delta87.org/2021/02/using-frontier-technology-detect-hidden-labour-abuses-agricultural-sectors-thailand/?lang=fr>



Ces travailleurs agricoles saisonniers passent en général deux à trois mois à travailler dans une ferme et reçoivent une avance sur salaire, ce qui rend compliqué « *de comprendre le lien entre les heures travaillées et le paiement reçu, en particulier si les employeurs font d'autres déductions pour les intérêts ou d'autres «coûts» (tels que la nourriture, les outils et le transport)*<sup>40</sup> ».

De plus, ce système d'avance sur salaire lie les travailleurs qui ne peuvent plus quitter leur emploi même en cas d'abus. Certains travailleurs ont ainsi suggéré qu'eMin puisse être utilisé pour documenter clairement leurs conditions de prêt et d'emploi, y compris les paiements et les coûts en nature (tels que la fourniture de nourriture et de transport). « *En documentant ces éléments critiques au début de la relation de travail sur un grand livre immuable, on apporterait plus de transparence et de confiance aux deux parties et on réduirait le risque d'exploitation*<sup>41</sup> » expliquent Leanne Melnyk de Diginex et Juliette Alemany de Verifik8.

Si le projet est encore en cours d'expérimentation, il s'agit bien d'un enjeu crucial de la traçabilité des chaînes

d'approvisionnement. Comme nous l'avons vu dans le chapitre « Chaîne d'approvisionnement & logistique », la transparence d'une chaîne d'approvisionnement ne vaut que si elle commence avec le premier maillon de la chaîne. Cette initiative rejoint ainsi celle de **Koa** dans le domaine de la récolte des fèves et de la pulpe de cacao, basée en Suisse et au Ghana, qui, en mars 2022 assure avoir rémunéré 2 250 petits agriculteurs ghanéens à hauteur de 263 000 euros et ayant également évité 390 tonnes de déchets alimentaires<sup>42</sup>.

Koa<sup>43</sup> forme les cultivateurs de cacao pour, en plus de récolter les fèves de cacao, traiter la pulpe auparavant mise au rebut, ce qui leur permet de gagner un revenu supplémentaire et d'être payés sans délai après le processus de production (voir Chapitre Chaîne d'approvisionnement & logistique).

Enfin, l'initiative **Workers Well-Being Program**<sup>44</sup> menée par la marque de jeans Levi Strauss & Co, accompagnée de ConsenSys, de l'Université de Harvard *Public Health Graduate School* et du *think tank* New America, vise à utiliser une blockchain pour collecter les résultats des enquêtes auprès des salariés de trois de

40 *Ibid.*

41 *Ibid.*

42 « Can Blockchain Fix the Chocolate Industry's Labor Issues ? », Jill Ettinger, Green Queen, Mar 24 2022, <https://www.greenqueen.com.hk/blockchain-cocoa-labor-issues/>

43 « Koa taking transparency to the next level with Seedtrace », Seedtrace, May 31 2022, [https://seedtrace-website.cdn.prismic.io/seedtrace-website/5270d7b5-7a21-408e-8661-beed0de6dd7e\\_Seedtrace\\_CaseStudy\\_KOA\\_01-zusammengefügt%2B%281%29.pdf](https://seedtrace-website.cdn.prismic.io/seedtrace-website/5270d7b5-7a21-408e-8661-beed0de6dd7e_Seedtrace_CaseStudy_KOA_01-zusammengefügt%2B%281%29.pdf)

44 « Blockchain for F chain for Factory Workers: A Study of Le ers: A Study of Levi's Worker WellBeing Program », Mary Basile, Golden Gate University School of Law GGU Law Digital Commons 3-25-2020, [https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1000&context=blockchain\\_law](https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1000&context=blockchain_law)

leurs entreprises mexicaines concernant leurs conditions de travail.

La blockchain mise en œuvre offre aux salariés un moyen de répondre anonymement à des enquêtes, permettant de faire remonter des informations critiques quant au niveau de la gestion de l'entreprise, sans autocensure. Les résultats sont stockés dans une blockchain privée, qui est néanmoins consultable par n'importe quel membre de l'entreprise. Les autorités mexicaines auront également la possibilité de consulter les résultats, étant membre du réseau.

Ce type de dispositif vise à aller au-delà de la législation du travail au Mexique

en s'appuyant directement sur des informations fournies par des travailleurs. Ce projet avant-gardiste, démarré en 2018, a connu un premier rapport d'impact courant 2020, reposant sur une évaluation qualitative du dispositif qui a concerné *« environ 195 000 travailleurs dans 118 usines réparties dans 16 pays, ce qui représente 65 % du volume de produits de l'entreprise<sup>45</sup> »*.

Du côté de l'entreprise Lévi-Strauss, les participants ont reconnu avoir eu une remontée d'information bien plus riche et documentée qu'à l'accoutumée, même si nous n'avons pas encore le recul nécessaire pour évaluer l'impact social de cette initiative.

---

45 « Levi Strauss & Co., Worker Well-being », Website, retrieved June 9, 2022, <https://www.levistrauss.com/how-we-do-business/worker-well-being/>



## ENJEUX ET QUESTIONS

Comment assurer une interopérabilité des certificats portant sur des diplômes ? Il s'avère qu'entre les deux méthodes utilisées par des *startups* et des entreprises pour garantir l'authenticité d'un diplôme ou d'un certificat, - horodater le document dans une blockchain publique ou s'appuyer sur un système d'identités décentralisées et d'attestations vérifiables, cette dernière semble offrir un cadre plus propice à l'interopérabilité des services, tout à la fois pour les apprenants, les établissements de formation et les employeurs ou tout tiers susceptibles de vérifier l'authenticité d'un diplôme.

L'Europe semble privilégier cette voie, notamment par les travaux de l'EBSI qui déploie un réseau de nœuds distribués pour permettre la certification des diplômes<sup>1</sup>.

Le marché du travail étant caractérisé par une relation employeur/employé, en quoi de nouvelles formes d'organisations décentralisées réinventent les relations de travail ou des communautés travaillant à un objectif commun ?

Si l'initiative Gitcoin semble prometteuse, il convient toutefois de préciser que le marché sur lequel elle opère est un marché déséquilibré en faveur de l'offre, c'est-à-dire des développeurs informatiques. Leurs compétences sont en effet rares, en particulier pour des projets *open-source*.

Ainsi, les développeurs informatiques se retrouvent dans une position dominante, ce qui rend leurs conditions « d'embauche » attractives. Quelles seraient les conséquences de l'adoption d'une telle décentralisation sur un marché du travail moins déséquilibré ?

Quant aux projets blockchains visant l'amélioration des conditions de travail, que ce soit par l'enregistrement des contrats ou par les enquêtes anonymes, que valent-ils lorsqu'ils sont construits sur des blockchains privées ? Est-ce que ce type de projets pourraient se développer sur des blockchains publiques ? Si oui, pourquoi des entreprises en concurrence accepteraient-elles de communiquer ce type d'information ?

<sup>1</sup> « Diploma Functional Scope Skip to end of metadata », Marta Pastor, Regina dela Eva, European Commission, May 26 2021, <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Diploma+Functional+Scope>

N'y verraient-elles pas une ingérence dans leurs affaires ou une transparence sur les conditions de travail des « premiers maillons » de chaînes de valeur, encore largement opaques, notamment

sur les conditions de travail de salariés employés dans des pays de l'hémisphère Sud ? Quels pourraient être les freins ou les facteurs d'adoption de ce type de projets ?

## GLOSSAIRE

**Altcoin** : Un Altcoin désigne toutes les crypto-actifs alternatifs au bitcoin. Depuis la création du premier bitcoin en 2009, le site [coinmarketcap.com](https://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<sup>1</sup>, 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*<sup>2</sup> ». 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