IDENTITÉ & PROPRIÉTÉ

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.

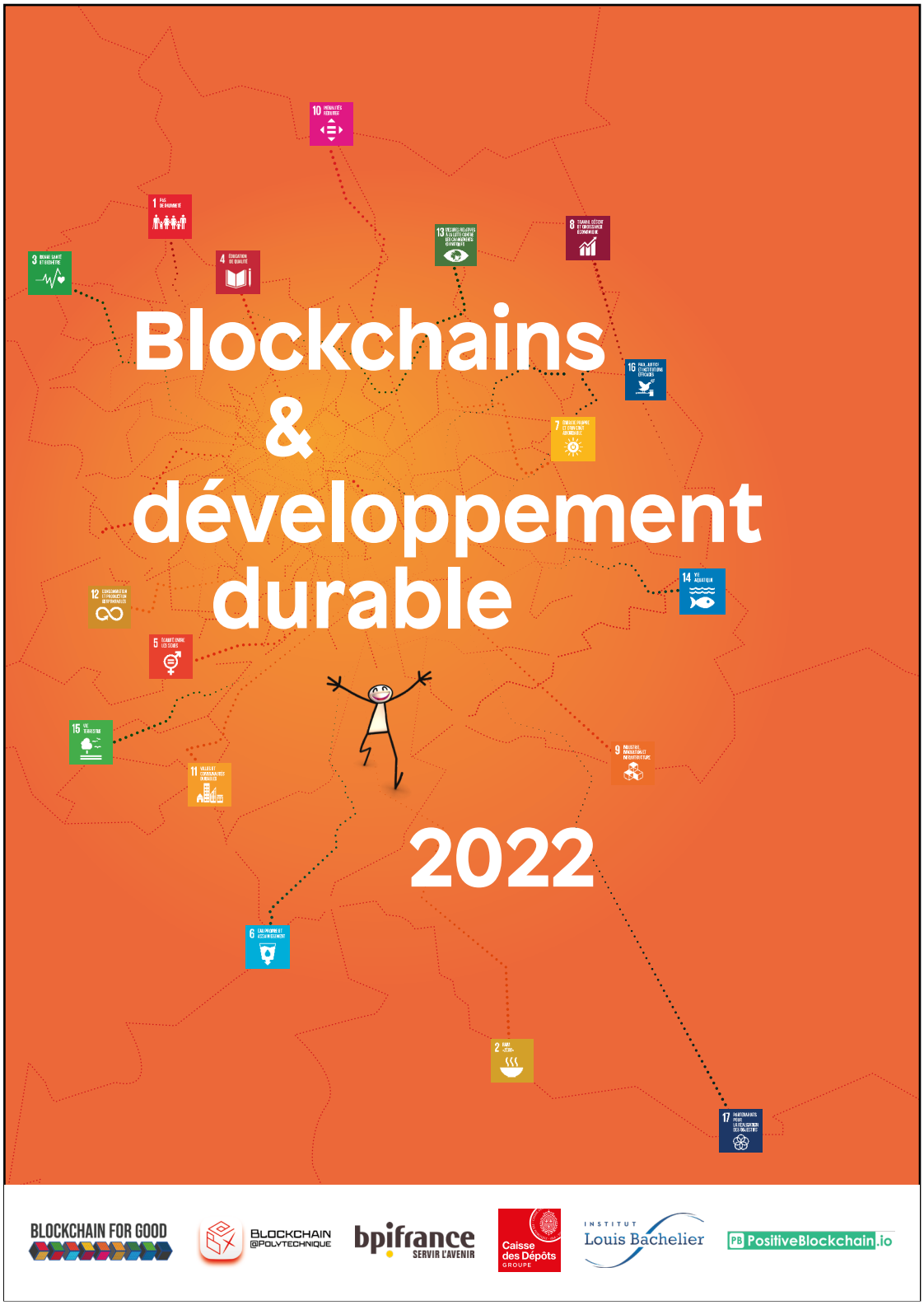
Bpifrance finance les entreprises - à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi leur activité export à travers une large gamme de produits. Conseil, université, 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.
Razali Samsudin, Chercheur indépendant, Éducateur, Co-fondateur de Sustainable ADA.

RELECTEURS CAHIER IDENTITÉ & PROPRIÉTÉ

Daniel Augot, Pierre Champsavoir, Martin Chazelle, Noémie Dié, Christophe Gbossou, Alejandro Gómez, Audran Gouis, Thibaud Huriez, Thibault Langlois-Berthelot, Paul Pflimlin, Paul Rivière.

TABLE DES MATIÈRES

IDENTITÉ ET PROPRIÉTÉ

Nombre de projets dans l'annuaire PositiveBlockchain.io : 99

Nombre de projets actifs : 71

Nom des projets actifs : Accredible ; Agrello ; Aid:Tech ; Archipels ; BenBen ; Bitfury Bermuda ; Bitfury Project in Georgia ; Bitnation ; Blockchain Helix ; BlockID ; brightID Bron.tech ; Chromaway ; Civic ; Crayonic ; Datafund ; Deloitte's Smart Identity ; Digiland Digital Bazaar ; Digitary ; EduCTX ; Empowa ; Golandregistry (UN in Afghanistan) Gravity ; Hala Systems ; ID2020 Alliance ; Iden3 ; Irisguard ; JOLOCOM ; Keeex Kilt ; Kleros ; Land LayBy ; LegitDoc ; Logion ; Mattereum ; Medici Land ; Netservice Open Time Stamps ; OpenCerts ; OriginStamp ; Polkadot ; Rohingya Project ; Safe Haven ; SecureKey and IBM ; Serto ; SESO ; ShareToken ; ShoCard ; Sovrin ; Spherity Spring Labs ; SpruceID ; Talao ; Thailand digital identity ; TiiQu ; Transcrypts ; Tykn Ubitquity ; Uniris ; UTU ; Veramo ; VERFiD Pet ; Verif-y ; veritise ; Vidchain ; WIN Woleet ; Wordproof ; Youbase / Cortex ; Zwei Space ; *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/

Qu'apportent les blockchains dans les domaines de l'identité numérique, la propriété foncière, la certification de documents officiels ? En quoi les blockchains renouvellent les relations entre les citoyens d'un pays et leurs administrations et services publics[1], les systèmes de gouvernance à l'échelle locale et globale, les systèmes de vote ?

Autant de sujets à propos desquels des projets blockchains remettent en cause des schémas traditionnels fondés sur une gouvernance centralisée et dont un thème nous semble à la fois central et transversal : l'identité numérique.

Partout dans le monde, la question de l'identité, et notamment de l'identité numérique, sont au cœur des enjeux de nos sociétés contemporaines qui se numérisent à marche forcée. Selon les Nations Unies, « *un enregistrement des naissances a eu lieu pour 73 % des enfants de moins de 5 ans dans le monde, mais pour seulement 46 % des habitants de l'Afrique sub-saharienne*[2] ».

1 Cette thématique fait l'objet d'un Chapitre dédié « Gouvernement & démocratie ».
2 « Goal 16: Promote just, peaceful and inclusive societies », United Nations, SDG website, retrieved May 9 2022, https://www.un.org/sustainabledevelopment/peace-justice/.

Alors que la population mondiale compte 7,9 milliards d'individus, un milliard de personnes[3] ne peuvent pas prouver leur identité, ce qui est déterminant, selon la Banque Mondiale[4], pour au moins dix des Objectifs de développement durable.

Comme nous l'écrivions en 2020[5], « *sans identité, pas de propriété d'un terrain, d'une maison ou d'un terrain agricole ; sans identité, pas de compte bancaire, donc pas de commerce ni de crédit, ni d'aides au développement sans intermédiaire ; sans identité, peu ou pas d'accès aux soins, si ce n'est ceux d'urgence, fournis lors de catastrophes ; sans identité, pas de scolarisation des enfants ; sans identité, pas de vote, ni d'accès à la justice* ». La cible 9 de l'Objectif de développement durable 16 vise expressément à garantir à tous « *d'ici à 2030, une identité juridique, notamment grâce à l'enregistrement des naissances* ».

De plus, dans les pays développés, l'identité, dorénavant numérique, est devenue l'essence du « *capitalisme de surveillance* », notion popularisée[6] en 2014 par l'économiste américaine Shoshana Zuboff, professeure émérite à la Harvard Business School.

Au capitalisme industriel du 20e siècle, emmené par le constructeur automobile Ford, succède une autre forme de capitalisme, de données, optimisé par Google dans les années 2000.

Le capitalisme de surveillance fonde son modèle sur l'enregistrement systématique de toutes les données personnelles des individus et de leurs interactions, la plupart du temps à leur insu, analysées à l'aide de puissants logiciels (Big data et intelligence artificielle) afin de vendre, à des annonceurs en ligne, une prédiction de comportement futur selon leur affiliation à un groupe démographique.

L'écueil est double. D'un côté, certains pays caractérisés par une défaillance des institutions n'arrivent pas fournir à leurs ressortissants un moyen de prouver leur identité et de l'autre, dans les pays développés, les individus bénéficient d'un anonymat très relatif, que ce soit pour des raisons commerciales et financières (capitalisme de surveillance), ou encore politiques et sécuritaires (lutte contre le terrorisme et blanchiment d'argent).

Dans les pays en développement, l'identité est d'autant plus cruciale qu'elle est le premier vecteur de reconnaissance juridique à partir duquel une personne pourra revendiquer la propriété d'un terrain et accéder à une multitude de services, notamment publics (parmi lesquels l'accès à la justice, à la sécurité sociale, le droit à l'éducation, le droit de vote etc.) ou privés (services financiers).

Quel intérêt présente l'usage de blockchains publiques dans les domaines de l'identité numérique, sur un registre personnel ou professionnel ? A quelle problématique répondent les projets blockchain portant sur la propriété foncière, le cadastre ou encore la certification de documents ?

Identité décentralisée

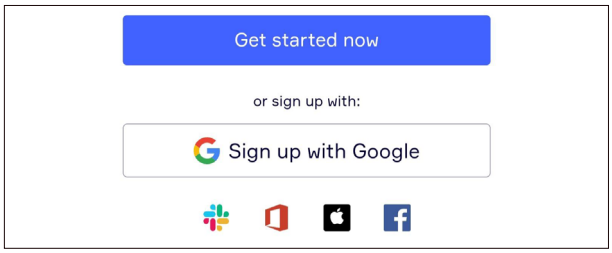
L'identité numérique est « *la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources*[7] ». L'apport des blockchains dans le domaine de l'identité numérique est d'inverser le modèle actuel fondé sur l'authentification et le contrôle d'accès, géré tout deux par une organisation, vers un modèle fondé sur la vérifiabilité d'attestations contrôlées par une personne.

Il s'agit donc de passer d'un modèle centralisé où l'utilisateur crée un identifiant et un mot de passe et dissémine ses informations personnelles auprès de chaque service, à un modèle décentralisé, où l'utilisateur reste maître de ses données personnelles.

Cela résout également d'intenses problèmes de sécurité liés à la centralisation des données en un même point, objet de piratages informatiques récurrents.

Un modèle décentralisé permet à une personne de fournir une preuve de son identité ou de l'une de ses facettes, comme son âge, auprès du service auquel il souhaite accéder.

Ce changement de paradigme de l'identité numérique amorce un tournant pour les grandes entreprises du web qui ont fondé leur modèle économique sur l'exploitation massive et centralisée des données personnelles à l'insu de leurs utilisateurs. Et notamment en tant que fournisseur d'identité fédérée, un compte Facebook ou Google, servant de solutions d'identification pour des services tiers (voir image *infra*).



La promesse de l'identité décentralisée est de permettre à l'utilisateur de prouver quelque chose sans révéler aucune information personnelle. Pour Thibault Langlois-Berthelot, doctorant en droit à l'EHESS, « *un modèle d'identité décentralisée propose à l'utilisateur de reprendre le contrôle sur sa propre identité en créant un ou plusieurs identifiants uniques nommés des «* identifiants décentralisés *», auxquels il va associer ses attestations d'identité vérifiables aussi nommés «* verifiable credentials[8] ».

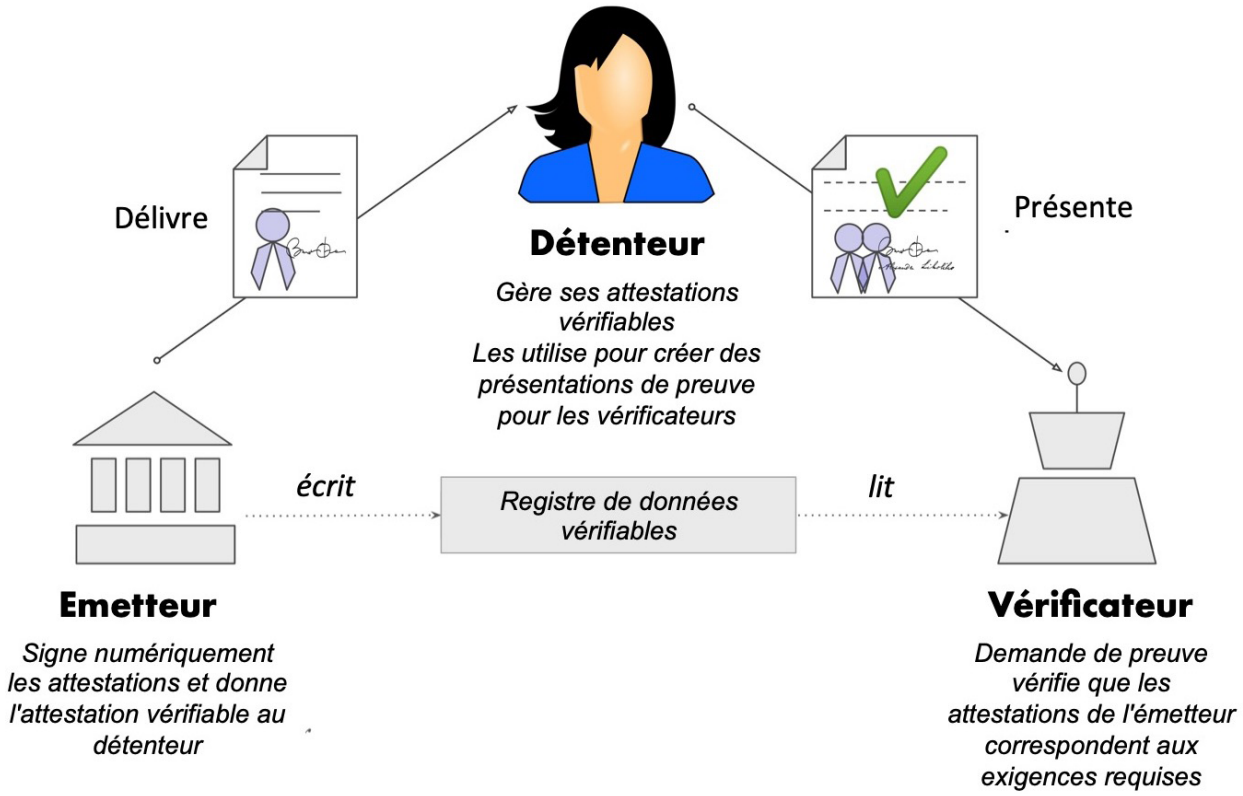
Ces identifiants décentralisés sont des standards informatiques qui normalisent de nouveaux mécanismes d'échange de données basés sur la cryptographie et des registres distribués. Ces standards, open source et publics sont en cours d'élaboration à l'échelle mondiale, notamment par le W3C, Trust Over Ip[9] affilié à la fondation Linux ou encore la Fondation Decentralized Identity[10].

A partir d'un identifiant décentralisé stocké dans un portefeuille d'identité*[11], une personne prouve, par l'intermédiaire d'« attestations vérifiables » qu'il sélectionne ce qu'il sait (diplômes, autorisation d'exercer un métier, certification), ce qu'il a (compte bancaire, citoyenneté), ce qu'il possède (terrain, résidence, propriété, véhicule), qui il est (taille, poids, âge), ce qu'il fait (emploi, passé ou présent), où il a été (participation à un évènement), s'il a été ou non vacciné contre la Covid 19 etc.[12].

Ces attestations vérifiables sont « *des certificats numériques standardisés qui facilitent l'échange et le partage d'informations en ligne, de manière souveraine et sécurisée*[13] ».

Un système d'identité décentralisé fait

8 « Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique », Thibault Langlois Berthelot, 27 octobre 2021, https://hal.archives-ouvertes.fr/hal-03314568
9 « About us », Trust Over IP Foundation, Trust Over IP Foundation website, retrieved May 9 2022, https://trustoverip.org/about/about/
10 « Our Focus », Decentralized Identity Foundation, DIF website, retrieved May 9 2022, https://identity.foundation/
11 Les mots marqués d'un astérisque* font l'objet d'une entrée dans le glossaire, en fin de rapport.
12 « An Introduction to Verifiable Credentials », Verifiable Credentials.io, retrieved May 9 2022, https://verifiablecredential.io/learn
13 Op. Cit. « Blockchain et souveraineté, les prémices d'une révolution de l'identité numérique », Thibault Langlois Berthelot, https://hal.archives-ouvertes.fr/hal-03314568



Attestations vérifiables, triangle de la confiance
Source : *Credentials, triangle of Trust* , Daniel H Hardman - CC BY-SA 4.0. Traduction Blockchain for Good
https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/VC_triangle_of_Trust.svg/2560px-VC_triangle_of_Trust.svg.png

interagir trois entités : (1) Un émetteur (*issuer*) émet un identifiant décentralisé (DID) à un détenteur (*holder*), (2) sur la base de cet identifiant, le détenteur (*holder*) présente des attestations (ou justificatifs, *verifiable credentials*) le concernant à un vérificateur (*verifier*), par exemple pour accéder à un service, (3) le vérificateur ou service vérifie ces justificatifs

- Le détenteur (*holder*) est une entité, comme un étudiant, une personne, un employé, qui acquiert, conserve un ou plusieurs identifiants décentralisés, suivant ses besoins et les services auxquels il veut accéder.
- L'émetteur (*issuer*) est une entité, comme une entreprise, une ONG, un gouvernement, une université, qui certifie certains champs de cette identité : nom, âge, âge, pays de naissance, avoirs bancaires, etc. Ces champs ne sont pas nécessairement tous présents dans un même DID, et une personne peut avoir plusieurs DIDs. Par exemple, un DID civique peut encoder l'état civil d'une personne, alors qu'un DID bancaire pourrait encoder des informations relatives à un numéro de compte. Sur la base d'un DID, son détenteur peut produire un justificatif, (attestation vérifiable, ou *verifiable credential*)

qui est l'énoncé d'un fait portant sur un ou plusieurs champs du DID, qui restent secrets. Par exemple, sur la base du DID civique un justificatif de majorité peut être fourni sans révéler son âge. Sur la base du DID bancaire, la solvabilité peut être prouvée sans révéler son nom ni le montant de son compte en banque. Cela est possible grâce aux preuves à divulgation nulle de connaissance* (*Zero Knowledge Proof* – ZKP).[14]

- Enfin, le vérificateur (*verifier*) est une entité, comme un employeur, les forces de l'ordre, un service administratif, qui reçoit une attestation vérifiable et la vérifie suivant la technique de vérification de preuves à divulgation nulle de connaissance.

En pratique un DID peut être vu comme un lien qui pointe vers un document complet contenant les champs du DID cryptographiquement protégés. Ce document est stocké dans un registre (Verifiable Data Registry) qui peut admettre divers degrés de centralisation selon qu'il est placé dans une blockchain ou d'autres types de base de données. Ce registre de données vérifiables sert d'intermédiaire indirect entre l'émetteur d'une attestation vérifiable et le vérificateur.

Le détenteur (holder) contrôle ainsi les informations qu'il choisit de partager sous forme d'attestations vérifiables et peut attester de tout ou partie de ses attributs d'identité sans que l'émetteur n'en soit informé.

Plutôt que de renseigner son nom, créer un login, un mot de passe et livrer des informations personnelles auprès d'un service, quel qu'il soit, le détenteur d'un portefeuille d'identité* ou *identity wallet* dispose d'attestations vérifiables à partir desquelles le service auprès duquel il souhaite prouver quelque chose vérifie que ce qu'il revendique est vrai. Ce nouveau paradigme d'identité décentralisée s'appuie de manière cruciale sur un cadre technique permettant de mettre en œuvre le principe de « la preuve à divulgation nulle de connaissance » proposé par Charles Rackoff, Shafi Goldwasser et Silvio Micali en 1985[15].

La preuve à divulgation nulle de connaissance permet de présenter des preuves de faits portant sur des données personnelles sans pour autant les révéler. « *Ces preuves ne révèlent aucune autre information que le fait que ces propriétés ou énoncés sont vrais* » explique Daniel Augot, Directeur de recherche à l'INRIA et enseignant à l'École polytechnique. Cette technologie est déployée nativement sur certaines

blockchains publiques comme ZCash, ou Monero, mais peut également l'être au-dessus de blockchains existantes comme zk.money sur Ethereum. Elle offre une grande diversité d'usages, notamment dans le domaine de la finance, de la santé ou encore de l'identité décentralisée et dont le dénominateur commun sera la confidentialité des données.

Ce modèle d'identité décentralisé résout les problèmes de la centralisation des données personnelles des individus par chaque entité avec laquelle il interagit en offrant un paradigme où l'individu reprend le contrôle sur son identité en garantissant tout à la fois une confidentialité de ses données et une transparence avec les entités avec lesquelles il interagit. Par exemple, les organisations humanitaires collectent les données personnelles de bénéficiaires d'aides dans de gigantesques bases de données indépendantes et souvent redondantes comme SCOPE du Programme Alimentaire Mondial (PAM), qui contient 20 millions d'identifiants, le système d'identification et d'enregistrement personnel de l'Organisation internationale pour les migrations[16] (OIM), qui contient également 20 millions d'identifiants, ou encore la solution mobile Last Mile de World Vision, qui contient 8 millions d'identifiants[17]. Ce modèle d'identité décentralisée est en cours de déploiement et testé par certains pays.

En avril 2021, le gouvernement Ethiopien 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[18]. 750 000 enseignants auront également accès au système. L'objectif est tout à la fois de fournir une identité numérique décentralisée aux étudiants et de développer le système d'éducation du pays, démarche qui s'inscrit dans le cadre de la stratégie de transformation numérique du pays, Digital Ethiopia 2025[19]. Selon le ministre de l'Éducation nationale, le gouvernement a également conclu un accord avec un fabricant chinois de tablettes informatiques, qui seront distribuées aux étudiants[20]. Ce programme, en cours de développement, utilise Atala Prism basée sur la blockchain publique Cardano, une « *solution d'identité décentralisée qui permet aux personnes de s'approprier leurs données personnelles et d'interagir avec les organisations de manière transparente, privée et sécurisée*[21] ».

16 Organisation internationale pour les migrations, consulté le 9 juin 2022, https://www.iom.int/fr
17 « The Next Generation Humanitarian Distributed Platform, Danish Red Cross, Mercy Corps, November 12, 2020, https://reliefweb.int/report/world/next-generation-humanitarian-distributed-platform
18 « Ethiopia's blockchain deal is a watershed moment – for the technology, and for Africa », Iwa Salami, May 20, 2021, https://theconversation.com/ethiopias-blockchain-deal-is-a-watershed-moment-for-the-technology-and-for-africa-160719
19 « A digital roadmap for the developing world », Blavatnik School of Government, Blavatnik School of Government website, June 24, 2020, https://www.bsg.ox.ac.uk/news/digital-roadmap-developing-world
20 « Ethiopian Education Minister Confirms Cardano Blockchain Partnership », Anna Baydakova & Marc Hochstein, coindesk.com, April 30, 2021, https://www.coindesk.com/business/2021/04/30/ethiopian-education-minister-confirms-cardano-blockchain-partnership/
21 « Powering the Trust Economy », Atala Prism, website, retrieved May 9, 2022. https://atalaprism.io/app

FlexID Technologies est une *startup* basée à Harare au Zimbabwe, créée en 2018 par Victor Mapunga originaire du pays et Haardik, originaire d'Inde. Tous les deux se sont rencontrés à l'Université de Yale puis se sont suivis au King's College de Londres. Début 2018, Victor Mapunga a souhaité ouvrir un compte bancaire au Zimbabwe. « *J'ai été choqué de voir un long formulaire à remplir, qui exigeait des informations très irréalistes, surtout dans un pays comme le Zimbabwe qui a un taux de chômage de 90%, ce qui signifie que la plupart des gens vivent dans l'économie* "informelle"[22] ». Parmi les pièces demandées, un bulletin de salaire ou une preuve de résidence, des documents que la majorité des Zimbabwéens sont incapables de fournir. C'est en partant de ce constat, notamment parce que l'impossibilité d'ouvrir un compte bancaire dépend en grande partie de l'absence de documents d'identité, que FlexFinTx fut créé quelques semaines plus tard.

FlexFinTx est une plateforme d'identité décentralisée auto-souveraine, construite sur la blockchain publique Algorand et assortie du portefeuille d'identité FlexID Wallet. Un utilisateur crée gratuitement un FlexID en utilisant un code USSD (un code généré à partir de son téléphone portable) ou *via* WhatsApp. L'identité numérique de l'utilisateur est stockée sur l'Interplanetary File System (IPFS)*, un système de stockage de fichiers distribués (voir Chapitre Contenus numériques & Arts), inscrite dans la blockchain publique Algorand de sorte que seul l'utilisateur est détenteur de sa clef privée. A partir d'une application sur son téléphone, ou par l'intermédiaire d'un portefeuille d'identité physique, les utilisateurs pourront prouver leur identité et accéder ainsi à un éventail de services parmi lesquels « *créer un compte bancaire, demander un prêt ou même renouveler son permis de conduire sans avoir à se rendre dans une agence physique*[23] ».

La plateforme FlexFinTx est construite sur les normes établies par le World Wide Web Consortium (W3C) pour les identités décentralisées et les justificatifs d'attestations vérifiables, garantissant une interopérabilité avec d'autres fournisseurs de services. Selon Victor Mapunga « *la plateforme est extrêmement peu coûteuse à mettre en œuvre pour les entreprises et les gouvernements. En Afrique, les entreprises et les gouvernements devraient débourser des millions de dollars pour développer de tels systèmes, parfois par le biais de procédures d'appel d'offres entachées de corruption et construites par des entreprises étrangères qui n'ont aucune connaissance du marché africain*[24] ». La solution a été récompensée par le World Economic Forum Tech Pioneer en 2021, à l'occasion duquel le Zimbabwe était représenté pour la première fois.

22 « How FlexID is using Algorand to tackle a $50B problem across Africa », Haardik, January 28, 2020, https://medium.com/flexfintx/how-flexid-is-using-algorand-to-tackle-a-50b-problem-across-africa-daa5916b07b3
23 *Ibid.*
24 *Ibid.*

Terrains et titres de propriété

L'accès au foncier, la preuve de son identité et l'opposabilité d'un titre de propriété sont des rouages fondamentaux de l'inclusion des personnes dans la société. En effet, l'actif foncier représente souvent, pour les plus défavorisés, la seule contrepartie pour non seulement accéder à des services financiers mais également témoigner de leur identité.

Dans les pays où il n'existe pas de registre de la propriété foncière, l'intérêt de mettre en œuvre une blockchain repose sur l'immuabilité du registre et la facilité avec laquelle il peut être interrogé. De plus, les outils de géolocalisation facilitent l'identification et le marquage des terres non répertoriées. Avec un cadastre numérisé, la dématérialisation des titres fonciers résout également le problème de la perte de documents papiers, en particulier en cas de catastrophes naturelles ou de conflits. Enfin, l'absence d'organe centralisé chargé de l'inscription et de la maintenance du registre permet d'apporter une réponse au problème de corruption de certains rouages de l'administration et notamment d'expropriations ou appropriations arbitraires.

La cible 4 de l'Objectif de développement durable 1 vise à ce que, « *d'ici à 2030, tous les hommes et les femmes, en particulier les pauvres et les personnes vulnérables, aient les mêmes droits aux ressources économiques et qu'ils aient accès aux services de base, à la propriété foncière, au contrôle des terres et à d'autres formes de propriété, à l'héritage, aux ressources naturelles et à des technologies et des services financiers adéquats, y compris la micro-finance* ». De plus, l'accès à la propriété et la sécurisation du foncier concernent directement l'Objectif de développement durable 5, visant l'égalité des sexes, afin que des réformes donnent aux femmes les mêmes droits que les hommes, notamment parce qu'elles représentent la part la plus importante de la main-d'œuvre agricole en Afrique ; et l'Objectif de développement durable 8, qui vise à « *promouvoir une croissance économique soutenue, partagée et durable, le plein emploi productif et un travail décent pour tous* ».

Le Ghana, le Bangladesh, l'Afghanistan, l'Inde mais aussi la Suède ou encore la Géorgie sont quelques-uns des pays s'intéressant de près aux technologies blockchains pour mettre en place un registre décentralisé de la propriété foncière. Comme nous l'avons détaillé en 2020 dans notre précédent rapport, la Géorgie, à travers l'Agence nationale du registre public, a sécurisé plus de 2 millions de titres fonciers dans la blockchain Bitcoin.

Fondée en 2015 par Emmanuel Buetey Noah, **BenBen** est une entreprise privée basée au Ghana dont l'objectif est de « *combler le fossé entre les détenteurs de droits fonciers et les acteurs du marché foncier* » en s'appuyant sur les technologies blockchains.

Lors d'un entretien accordé au Centre technique de coopération agricole et rurale (CTA), Emmanuel Buetey Noah explique que « *bon nombre d'États africains ne disposent toujours pas d'un système offrant un accès sûr et fiable aux marchés fonciers. Ceci s'explique principalement par le manque de transparence et d'accès à des données fiables sur les marchés fonciers – une conséquence des registres publics de mauvaise qualité et surchargés, ainsi que de la concurrence entre plusieurs régimes fonciers. En outre, seulement 20 % des transactions foncières seraient conclues de manière formelle. Par conséquent, 80 % des activités sur le marché foncier ne sont ni connues, ni documentées* ».

BenBen tâche d'agréger les données concernant les transactions publiques à la fois formelles et informelles, afin d'adresser les défis liés à l'acquisition de terres au Ghana qui se heurte « *à des difficultés telles que les ventes multiples, les nombreux frais non officiels, les bureaucraties inutiles, l'intrusion d'intermédiaires non qualifiés et le manque de transparence, entre autres* ». Le travail d'agrégation de données mené par BenBen rassemble des données foncières qui peuvent être utilisées par différents acteurs du marché. Afin d'améliorer l'accès à ces données, la version actuelle de la solution de BenBen propose également des fonctionnalités visant à faciliter les demandes et l'enregistrement des transactions foncières pourvues de garanties par différents acteurs du marché foncier ghanéen. L'architecture technique de BenBen repose sur l'utilisation d'un registre distribué, visant à garantir l'intégrité et l'immutabilité des données sur la propriété foncière pour à la fois simplifier les procédures administratives mais également offrir ce service à des coûts abordables.

Le prototype décrit par BenBen s'appuie sur la blockchain publique Bitcoin et sur l'Interplanetary File System (IPFS)*, en hachant les données liées aux transactions et en les ancrant dans la blockchain Bitcoin, ce qui permet « *garder une trace immuable et accessible publiquement de blocs qui renvoient à différents documents et transactions foncières réalisées via la plateforme. De plus, les capacités de stockage de l'IPFS nous permettent de proposer un protocole sécurisé de partage des données, de stocker des données cadastrales immuables (relatives à la propriété des terres), et de prévenir la duplication des registres et documents sur les transactions foncières* ».

En Afghanistan, l'Office of Information and Communications Technology (OICT) des Nations Unies, en partenariat avec l'ONU Habitat testent, depuis 2019, un registre foncier numérique s'appuyant sur un registre distribué : **goLandRegistry** pour « *government office Land Registry* ». Partant du constat que « *80 % des propriétés urbaines ne sont pas enregistrées auprès des autorités locales ou nationales* » et que les questions de

propriétés foncières sont « *à l'origine de conflits armés et d'abus des droits de l'homme* », les organisations développent un « *système conçu pour enregistrer tous les documents de propriété sur une blockchain, ainsi que pour délivrer des certificats d'occupation* », ce qui permettra aux propriétaires de démontrer de manière indépendante l'authenticité des certificats d'occupation à l'aide d'un outil de vérification open source et accessible à tous.

goLandRegistry s'appuie sur la blockchain hybride LTO Network, qui repose tout à la fois sur un réseau public et sur un réseau privé. Les organisations enregistrent des transactions entre elles, de manière privée, afin d'ordonner temporellement des événements dont notamment la signature de contrats. Certaines de ces informations sont ensuite ancrées sur une blockchain publique, ce qui permet de consigner ce qu'elles ont fait entre elles. Les deux organisations des Nations Unies ont ainsi développé un système informatique dont l'objet est d'enregistrer et vérifier les actes de cadastres et de suivre le financement foncier provenant de pays extérieurs.

Selon les Nations Unies, le programme goLandRegistry contribue aux Objectifs de développement durable 1, 5, 11, 13, 15, 16 et 17 et aurait eu vocation à s'étendre à d'autres pays. Mais depuis le retour au pouvoir des talibans en septembre 2021, nous ne savons pas ce qu'il adviendra de ce programme.

> Basée à Amsterdam, LTO Network a développé une plateforme qui enregistre entre 80 et 100 000 transactions par jour et est aujourd'hui utilisée par le gouvernement hollandais, le gouvernement afghan, Heineken, les Nations Unies, Airbus, Bosch, Dekkra ou encore IBM. LTO déploie un système de blockchain hybride, combinant l'utilisation d'une blockchain publique dont le mécanisme de consensus est basé sur la preuve d'enjeu et des blockchains privées, contrôlées par des organisations, qui opèrent leur propre mécanisme de consensus en s'appuyant sur une version hachée des transactions enregistrés sur la blockchain publique.

Au Bangladesh, **Digiland**, créé en 2018, s'attache à « *numériser le système de registre foncier en développant une plateforme de propriété transparente et immuable basée sur la technologie blockchain* ». L'enjeu est de taille puisque le Bangladesh est l'un des États au monde le plus densément peuplé, avec 165 millions d'habitants, sur une superficie aussi petite que l'État de New York, et 22 millions dans la seule ville de Dhaka. « *Depuis 2018, Digiland travaille avec le gouvernement bangladais pour mettre en place un registre de propriété sur le même modèle que celui développé en Géorgie, c'est en à dire en interfaçant le système avec l'administration et le gouvernement afin que les titres de propriété soient reconnus et donc opposables à tous* » explique Niklas Friese, l'un de ses fondateurs.

Parmi les difficultés rencontrées par Digiland figurent notamment le fait que peu de Bengladais disposent d'une pièce d'identité. De plus, les règles d'héritage et de transmission des terres dépendent en grande partie de la religion et certaines terres, notamment gérées par des coopératives agricoles, sont administrées par un chef de village plutôt que par les agriculteurs. Le registre de propriété consiste à enregistrer les titres de propriété tout à la fois dans la blockchain publique Ethereum et une sidechain* privée.

Certification et notarisation

Au-delà de l'identité numérique et du registre foncier, il est utile de pouvoir prouver l'authenticité et l'existence de documents à un moment précis comme un contrat, un diplôme, un contrat de bail, une photo, un acte juridique etc. Jusqu'à présent, ce processus a toujours nécessité l'intervention d'un officier public ou d'une autorité tierce certifiant l'existence et l'intégrité d'un document.

Lorsque le document est certifié par un officier public, il est un acte authentique, c'est-à-dire opposable à tous. Un acte authentique est « *celui qui a été reçu par des officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises*[25] ». Ces officiers publics ont un rôle de tiers certificateur aux yeux de la loi et de tous comme, en France, les notaires, les huissiers de justice, les commissaires-priseurs ou encore les greffiers des tribunaux de commerce.

Lorsque deux entreprises signent un contrat, par exemple un accord de confidentialité, elles peuvent prévoir de certifier le document afin d'anticiper de futurs litiges. S'il s'avère qu'une des parties transmet des informations à un tiers, elle pourrait prétendre l'avoir fait avant de signer l'accord. La date de signature, l'intégrité du document et la signature du contrat revêtent alors une importance cruciale. Pour certifier l'accord de confidentialité, les parties auraient pu s'appuyer sur un tiers de confiance dont l'objet est de fournir ce service d'horodatage certifié, appelé aussi une « Autorité de certification des temps » (de l'anglais *Timestamping Authority*, TSA). L'horodatage certifié (en anglais Trusted timestamping) est donc un système qui permet de conserver la preuve de l'existence d'un document et de son contenu à une date précise et qui implique qu'une fois le document daté et signé, il est impossible à quiconque, pas même son propriétaire, de le modifier.

Passer par un tiers de confiance a un coût ; être un tiers de confiance également. Par exemple, une université ou une école qui délivre des diplômes doit tenir un registre des diplômés, et être en mesure d'être contactée par des entreprises et des organisations qui souhaitent vérifier qu'une personne est effectivement diplômée de l'école ou l'université en question. Enregistrer l'empreinte d'un diplôme dans une blockchain publique permet de considérablement

Hacher un texte via l'algorithme SHA-256

Le SHA-256 est une norme de hachage qui permet de faire correspondre à une donnée binaire quelconque, une empreinte de 64 caractères hexadécimaux unique. Une fonction de hash est une 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.
Prenons l'exemple suivant. Si l'on hache le texte « Blockchain et développement durable », le résultat du hash sera le suivant : faf60b6b9dc3561f167f9b88ab2c8229bb883da79afe4f11b22be7dda692618c. Si l'on modifie le texte à hacher en enlevant l'accent sur le mot développement « Blockchain et developpement durable », le résultat du hash sera le suivant : 0214a2148333104bf8ff3e8108bee1944b9a614727f4871ec6473b5d5f43fd38.
Il est donc impossible de retrouver le message d'origine à partir du hash. En revanche, si l'on hashe à nouveau « « Blockchain et développement durable », on retrouvera toujours le même nombre hashé : faf60b6b9dc3561f167f9b88ab2c8229bb883da79afe4f11b22be7dda692618c, prouvant ainsi que le texte n'a pas été modifié.
Il est possible de hasher une phrase, un mot de passe, ou encore L'Iliade et l'Odyssée *in extenso* qui fait plus de 700 pages, cela donnera toujours une empreinte unique de 64 caractères hexadécimaux. L'intérêt d'une fonction de hachage est donc qu'elle ne s'applique que dans un sens : le nombre hashé 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.

simplifier la procédure pour vérifier l'authenticité d'un diplôme. Nous abordons en détail cette problématique dans le chapitre « Education et emploi ».

Les blockchains publiques comme Bitcoin, Ethereum ou Tezos sont des registres universels, ouverts et accessibles à tous et dont les données sont immuables. Des services de certifications de documents se sont ainsi créés en s'appuyant sur ces blockchains publiques, parmi lesquels Woleet, KeeeX, OriginStamp ou encore OpenTimestamps. Woleet est une « *plateforme qui permet de garantir l'intégrité et la provenance des données en liant tout type de contenu numérique à des transactions Bitcoin immuables*[26] ». Ce n'est pas le document en lui-même qui est enregistré dans une blockchain publique mais le document haché (voir encadré). Les documents ainsi certifiés

26 « Woleet : Fournisseur d'accès à la vérité numérique », Vincent Barat, Gilles Cadignan, Livre blanc, 30 Juin 2017, https://www.woleet.io/wp-content/uploads/2019/06/Woleet-WP-0.3-FR.pdf

peuvent être vérifiés sans tiers, partout dans le monde et à tout moment.

En France, la Caisse des dépôts et consignations, La Poste, Engie et EDF ont créé Archipels, qui propose, selon son CEO, Hervé Bonazzi, « *une infrastructure souveraine qui permet de gérer et de vérifier l'identité numérique. C'est une plateforme de confiance numérique qui certifie sur la blockchain des documents, des données et des informations sur des individus ou des entreprises et qui rend vérifiable leur authenticité* ».

Développé avec Vialink[27], un acteur français de l'automatisation du traitement des dossiers clients (*Know Your Customer*) pour la banque, l'assurance et l'immobilier, Archipels a lancé début 2021 un premier service de contrôle de l'authenticité des justificatifs de domicile, à propos desquels les tentatives de fraude sont en constante augmentation[28].

« *Notre solution vise à créer une infrastructure de confiance globale mise à disposition de tout tiers désirant vérifier l'authenticité d'un document. Notre blockchain est privée et permissionnée, ce qui signifie que les acteurs validant les transactions sont des tiers de confiance identifiés et autorisés à le faire. Nous avons une maîtrise totale de l'origine des documents certifiés*[29] », explique Hervé Bonazzi. La blockchain étant privée et permissionnée, elle s'appuie sur un algorithme de consensus basé sur la Preuve d'autorité* (Proof of Authority), où quelques acteurs ont la charge de valider les transactions et de mettre à jour le registre distribué entre eux[30]. Les clients d'Archipels sont des banques, les greffiers des tribunaux de commerce ou encore des professions réglementées qui ont l'obligation de vérifier le justificatif de domicile.

En novembre 2021, Archipels a consigné 40 millions de ces justificatifs, garantissant leur authenticité auprès de leurs clients. La certification documentaire proposée au Conseil national des greffiers des tribunaux de commerce permettra aux greffiers, en 2022, de vérifier, *via* une API*, l'existence du siège des entreprises immatriculées au Registre du commerce et des sociétés (RCS).

L'intérêt d'utiliser une blockchain privée et permissionnée serait de gagner en auditabilité entre quelques acteurs de confiance et d'optimiser les coûts liés à leur coordination. La Chambre des Notaires de Paris a développé un premier pilote de certification et d'horodatage de document en 2019, sur la plateforme *open source* Hyperledger Fabric. Depuis juillet 2020, la Chambre des Notaires de Paris développe un registre distribué,

27 « Qui sommes-nous ? », Vialink, consulté le 9 mai 2022, https://www.vialink.fr/fr/qui-sommes-nous/lentreprise-vialink-qui-sommes-nous-2/
28 « Onfido's Identity Fraud Report 2020 »,Onfido, https://onfido.com/landing/fraud-report-2020/
29 « La blockchain pour certifier des documents personnels », Philippe Richard, 4 mars 2021, https://www.techniques-ingenieur.fr/actualite/articles/la-blockchain-pour-certifier-des-documents-personnels-90033/
30 « Notre Manifeste », Archipels, consulté le 9 mai 2022, https://en.archipels.io/notre-manifeste

à côté du logiciel métier traditionnel déjà utilisé par la profession, Espace Notarial, dont l'objet est de dématérialiser les dossiers, les échanges et les signatures avec leurs clients et entre notaires. La blockchain, privée et avec permission, servira, entre autres, à échanger des fichiers très volumineux, tracer et certifier des documents électroniques et tracer les actions des sociétés non cotées, application connexe développée par le Fonds d'Innovation de la Chambre des Notaires de Paris.

Gravity, créé en 2017, est une plateforme de cloud décentralisé à travers laquelle des personnes reçoivent, conservent et partagent des données vérifiables dans un portefeuille numérique sécurisé dont ils ont le plein contrôle. Construit sur la blockchain publique Tezos, Gravity développe trois types d'usages liés à l'identité décentralisée : Les solutions d'aide humanitaire, les solutions d'identité gouvernementale et les solutions de prêt.

Gravity participe notamment au projet DIGID, pour DIGnified IDentities, initié en 2021 avec l'aide de la Fédération internationale de la Croix-Rouge (IFRC), Innovation Norvège, la Croix-Rouge norvégienne, Save the Children Norvège, le Norwegian Refugee Council et le Norwegian Church Aid[31]. Le projet « *s'efforce de redonner le contrôle et la propriété des données personnelles aux individus, et en même temps d'augmenter la collaboration entre les ONG et leurs bénéficiaires, avec le consentement de l'utilisateur comme clé* ». La Croix-Rouge kényane (KRCS) rencontre des difficultés pour effectuer des transferts d'argent à environ un quart des bénéficiaires visés par ses programmes d'aide. Ces personnes ne peuvent en effet pas justifier d'une pièce d'identité alors que le fournisseur d'argent mobile M-PESA, utilisé normalement par l'ONG kényane, en requiert une pour créer un compte.

En avril 2021, la Croix-Rouge locale et RedRose[32] ont ainsi testé la solution de Gravity auprès de premiers bénéficiaires dans un environnement contrôlé, en milieu rural et en milieu urbain. N'importe qui peut bénéficier d'une identité décentralisée, y compris ceux qui n'ont ni smartphone, ni téléphone basique (feature phone*) ; l'ONG remplit un profil, une seule fois, sur la plateforme, puis remet à la personne un QR code imprimé puis laminé.

Les premiers retours d'expérience des ONG témoignent d'un gain de temps, que ce soit de la part des bénéficiaires ou du personnel sur le terrain. « *Le temps de vérification d'un bénéficiaire prend approximativement une minute*[33] » témoigne une ONG ayant testé la solution. Le système permet également de réduire drastiquement les frais financiers de 85 à 94%, « *le coût par bénéficiaire d'un QR code imprimé et laminé est de 0,30 USD, contre 2 à 5 USD pour la carte à puce qu'utilise généralement la Croix-Rouge kényane*[34] [le service de transferts

31 « Q&A with Gravity's lead engineer: François Guérin », Shiyao Zhang, september 23, 2021, https://medium.com/gravity-earth
32 Redrose est une organisation à but non lucratif britannique créée en 2014 qui développe une solution de transfert d'argent électronique pour le secteur humanitaire. https://redrosecps.com/
33 Gravity Earth, Medium, https://medium.com/gravity-earth
34 *Ibid.*

d'argent via mobile M-PESA - N.D.L.R.] » indique Gravity.

Gravity participe d'un écosystème distribué, normé, basé sur la cryptographie et dont le fonctionnement est privacy by design[35]. Un monde aux antipodes des pratiques habituelles des Organisations internationales d'aide humanitaire. Toutes utilisent aujourd'hui des logiciels de management de l'identité différents, chacun reposant sur la constitution de base de données centralisées, reliées au système bancaire traditionnel, international et local ou aux opérateurs de télécommunications locaux. Et dont la procédure d'inscription des bénéficiaires doit recommencer à chaque nouveau programme, y compris au sein d'une même ONG.

La proposition de Gravity est de « *créer un identifiant décentralisé qui pourra ensuite être utilisé avec les autres programmes d'aides de l'ONG et avec d'autres ONG, ce qui auparavant était impensable*[36] » explique Sharanya Thakur, chef de projet chez Gravity.

S'est ainsi posée la question de l'interopérabilité de « *l'explorateur d'identifiant décentralisé* » que propose Gravity. Un explorateur de blockchain est un logiciel en ligne permettant de visualiser les écritures ancrées sur un réseau blockchain. Dans le cas de Gravity, l'explorateur de blockchain permet aux ONG de vérifier l'identité ou l'un des attributs de l'identité d'une personne. Gravity s'est assuré de l'interopérabilité entre différentes blockchains et différents protocoles, en s'appuyant sur un explorateur générique, open source, plus ouvert que celui initialement développé en interne, et surtout interopérable avec la blockchain publique Tezos et d'autres systèmes d'identité décentralisés.

L'intérêt pour les ONG est de pouvoir vérifier, à partir d'un seul outil en ligne, l'identité décentralisée d'une personne indépendamment de la blockchain et du protocole utilisé. Ainsi, en juillet 2021, Gravity et Tykn, une entreprise du secteur humanitaire créé à Amsterdam au Pays-Bas en 2016, ont annoncé[37] une collaboration pour tester l'interopérabilité de leurs solutions d'identité décentralisée. Ils ont réalisé une preuve de concept d'interopérabilité entre le protocole d'identification numérique de Gravity construit sur la blockchain publique Tezos et le portefeuille d'identité de Tykn construit sur la blockchain publique Sovrin, dans le cadre du projet DIGID (Dignified Identities in Cash Programming) au Kenya.

35 *Privacy by design* : Ann Cavoukian, ancienne Commissaire de l'information et de la protection de la vie privée de l'Ontario, au Canada et inventrice de la *privacy by design* qui signifie que la vie privée doit être prise en compte dès la conception d'un logiciel, et non pas à travers une régulation intervenant *a posteriori*. *In* Ann Cavoukian, Privacy By Design. The 7 foundational principles. Privacybydesign.ca, Jan 2011, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

36 Entretien avec Sharanya Thakur, décembre 2021 – Association Blockchain for Good.

37 « Gravity, Tykn advancing interoperability of two decentralized identity solutions for the humanitarian sector », Charissa Ng Svenningsen, July 27, 2021, medium.com/gravity-earth/

Gravity travaille également avec la Digital Lending Association in Kenya[38] (DLAK), une association de prêteurs numériques au Kenya. Un prêt numérique est un processus de prêt entièrement dématérialisé et qui ne nécessite donc pas de passage par une banque ou un établissement financier physique.

En forte croissance en Inde mais aussi en Afrique, le prêt numérique au Kenya recense à lui seul 49 opérateurs[39]. L'association DLAK, lancée début 2019 par onze membres fondateurs dont Tala, Alternative Circle, Stawika Capital, Zenka Finance, Okolea, Lpesa, Four Kings Investment, Kuwazo Capital et Finance Plan, rassemble aujourd'hui quelque 11 millions d'emprunteurs dans le pays. Gravity fournit une solution d'identité décentralisée à l'association DLAK pour les applications de prêt et a déployé une plateforme de partage de données pour la souscription de crédit en temps réel.

Enfin, Gravity travaille avec la Chambre d'industrie de Gaziantep en Turquie et le Programme des Nations Unies pour le développement (PNUD) pour déployer leur solution d'identité décentralisée auprès des réfugiés syriens qui participent à des programmes de formation.

La problématique est la suivante. « *Des centaines d'organisations proposent des formations à quatre millions de réfugiés syriens en Turquie. Cependant, en l'absence de registres centraux ou de partage de données : (1) il n'y a pas de visibilité sur le nombre de bénéficiaires qui ont été atteints et (2) il est impossible de fournir la bonne formation à la bonne personne au bon moment* » explique Allen Walter de Tezos[40].

Le projet avec Gravity consiste ainsi à fournir à chacun des bénéficiaires des « *titres d'éducation vérifiables, basés sur des certificats numériques*[41] » déployés sur la solution d'identité décentralisée. Fin 2021, Gravity comptait 3 000 personnes à travers le Kenya et la Turquie inscrites sur le mainet* de la plateforme Gravity[42], c'est-à-dire disposant d'un identifiant décentralisé (DID voir *supra*) sur leur blockchain publique.

38 « Building the Future of Digital Lending », The Digital Lenders Association of Kenya, retrieved May 9 2022, dlak.co.ke/
39 « State of Digital Lending in Kenya - 2021 », Reel Analytics Ltd, August 2021, https://www.dlak.co.ke/uploads/1/9/8/3/19835783/2021-reelanalytics-digital-lending-research-report.pdf
40 « Gravity: A Decentralized Solution To Create Trusted Private Digital Identities For Real-Life Use On Tezos », Allen Walters, April 17, 2021, https://xtz.news/latest-tezos-news/gravity-a-decentralized-solution-to-create-trusted-digital-identities-for-real-life-use/
41 *Ibid.*
42 *Ibid.*

ENJEUX ET QUESTIONS

L'identité numérique décentralisée est un nouveau paradigme encore en construction, évoqué pour la première fois en 2012[43]. Il se développe en même temps que perdure celui de l'identité numérique centralisée et de l'identité numérique fédérée, dont les promoteurs ont beaucoup à perdre. En effet, l'un des enjeux majeurs du déploiement d'un paradigme d'identité décentralisée vient des résistances de la part des acteurs privés dont le modèle repose sur l'identification de leurs utilisateurs, notamment à des fins publicitaires et commerciales.

Rod Hall, analyste chez Goldman Sachs observe ainsi qu'à l'heure actuelle « *l'identité numérique n'appartient pas à l'utilisateur, mais est plutôt fournie par une myriade de sites web et de gardiens* (...) *Au lieu de se connecter avec Facebook, Google ou Apple, un avenir orienté blockchain permettrait aux utilisateurs de se* "connecter soi-même" *sans avoir besoin d'une tierce partie pour confirmer l'identité*[44] ». La position des éditeurs de navigateurs web, Mozilla, Alphabet, ou Apple est sans équivoque. Fin 2021, le W3C a procédé à un vote portant sur l'opportunité de recommander la spécification pour les « identificateurs décentralisés » DID. Le vote au sein du W3C étant secret, les seuls commentaires publics viennent de Tantek Çelik, en charge des standards Web au sein de Mozilla Corporation et font également référence aux commentaires de Microsoft et de Google. Mozilla reproche à la spécification DID de n'avoir « *aucune opérabilité pratique*[45] », ce qui « *encourage la divergence plutôt que la convergence*[46] » et pourrait, dans certains cas, favoriser la centralisation des données.

43 « *Évoquée pour la première fois par la formulation 'Sovereign Source of Authority' en 2012, l'identité décentralisée connaît une accélération majeure de son attrait et de son adoption depuis 2017* », Thibault Langlois-Berthelot. Proposition d'une taxonomie française pour l'identité décentralisée. Publié le 22 octobre 2021, https://hal.archives-ouvertes.fr/hal-03398096

44 « Ways blockchain can deactivate Facebook, Apple and Google's business models, per goldman », Tiernan Ray, The Technology Letter, December 20, 2021, https://www.thetechnologyletter.com/the-posts/ways-blockchain-can-deactivate-facebook-apple-and-googles-business-models-per-goldman

45 « Are Mozilla, Apple, Google opposing user control over identity ? | Billionaire kicks off effort to challenge social networks with "distributed" identity », Privacy Beat, September 24, 2021, https://itega.org/2021/09/24/why-mozilla-is-opposing-user-control-over-identity-billionaire-kicks-off-effort-to-challenge-social-networks-with-distributed-identity/

46 *Ibid.*

Mozilla affirme également que la prise en charge par DID des technologies de registres distribués telles que la « *blockchain* » pourrait conduire à « *un traitement énergivore contribuant au changement climatique mondial*[47] », et de conclure que cette norme ne doit pas devenir une recommandation.

Se pose également la question de savoir quelle est l'entité (entreprise, gouvernement, organisation décentralisée, *startup*…) qui met en place un système d'identité numérique décentralisée.

Est-ce qu'une identité auto souveraine fournie par un État sera reconnue au sein d'un autre écosystème et inversement ? Est-ce qu'un État pourrait reconnaître une identité souveraine qui ne provient pas d'eux ? Une certitude pour assurer cette interopérabilité, l'identité numérique décentralisée devra tout à la fois s'appuyer sur des standards et un langage commun et le W3C joue un rôle de premier plan à ce sujet[48]. Il s'avère que mettre en place une solution d'identité décentralisée au niveau régalien dépend largement de la maturité des services publics du pays : il est bien plus simple pour un pays qui ne dispose pas d'un système d'identité de basculer progressivement vers un modèle d'identité décentralisée et plus complexe à envisager de la part d'un pays qui s'appuie sur des services publics matures.

Autre question, comment déployer une solution d'identité décentralisée dans des pays dont les infrastructures de réseau, la connectivité à Internet et le taux d'équipement en téléphonie et smartphone ne sont pas développés, ou tout du moins laissent des gens de côté ? IN Groupe et UNICEF France tentent de répondre à cette problématique en proposant DID4ALL « *une identité numérique dans un contexte de faible connectivité, d'équipement technologiquement limité* [feature-phone*]*, d'illettrisme et d'illectronisme*[49] ». Le projet vise tout particulièrement à fournir une identité aux 166 millions d'enfants dans le monde qui ne bénéficient pas d'une existence juridique dans leur pays. L'objectif de DID4ALL est de combiner une technologie de reconnaissance vocale, une blockchain et les systèmes de télécommunication en proposant un système qui « *ne dépend pas d'un accès à internet, est accessible par tous, même les personnes qui ne savent pas lire ou écrire, est fiable, car reposant sur l'identification par la voix qui est un facteur d'authentification*

47 *Ibid.*
48 « Verifiable Credentials Data Model v1.1 Expressing verifiable information on the Web W3C Recommendation », November 9, 2021, https://www.w3.org/TR/vc-data-model/
49 Perrine de Coëtlogon, Marc Durand, Maxime Jeantet, Claire Génin, Romuald Ramon, et al.. Les technologies blockchain au service du secteur public. [Rapport de recherche] Université de Lille (2018-2021). ffhal-03232816v2f https://hal.archives-ouvertes.fr/hal-03232816/document#page=50

unique et, enfin, est sécurisée puisque les données sont stockées de façon distribuée puis horodatée sur une blockchain[50] ».

L'identité numérique décentralisée pose également la question de savoir comment fait une personne qui perdrait le dispositif numérique sur lequel est enregistrée ses attestations vérifiables*. Si elles sont stockées sur un téléphone portable et que ce dernier est perdu ou détruit, comment les récupérer ?

Avec les solutions d'identité décentralisée reposant sur des « HD wallet[51] » (*hierarchical deterministic wallet* - porte-clé déterministe hiérarchique), comme notamment celle proposée par Atala Prism, une personne peut restaurer son portefeuille d'identité* en renseignant une « phrase mnémotechnique* », en anglais « *seed phrase* », générée lors de la création d'un portefeuille d'identité sur une blockchain. Il convient donc, pour un utilisateur, soit de noter cette phrase mnémotechnique (ce qui constitue alors un risque de se faire pirater son identité), soit de devoir la retenir par cœur, au risque de ne jamais pouvoir accéder de nouveau à son portefeuille d'identité*.

Dans le domaine des registres fonciers décentralisés, notamment en Afrique, comment concilier une approche individualiste et occidentale d'un registre foncier avec la culture du pays où ce type de registre est mis en place ? Cette question prend tout son sens dans un contexte où interviennent des acquisitions récentes de terres importantes et engendrent des critiques sur les systèmes de gouvernance foncière. Au Ghana par exemple, les chercheurs Prince Donkor Ameyaw et Walter Timo de Vries de la Technische Universität München en Allemagne rapportent que « *le principe primordial pour toutes ces catégories de terres coutumières est que la terre appartient collectivement aux membres des communautés, mais que la gestion de la terre (et les décisions concernant son allocation et son utilisation) sont prises par les autorités coutumières au nom de ses membres. Selon certaines traditions au Ghana, la terre est gérée par les chefs coutumiers au nom des membres passés, actuels et futurs des communautés*[52] ».

La question de savoir comment concilier le droit coutumier avec un registre distribué reste donc entière.

---

50 *Ibid.*

51 « HD wallet » = *hierarchical deterministic wallet* (en français, porte-clé déterministe hiérarchique). Décrit par Gregory Maxwell dans la Bitcoin Improvement Proposal (BIP) 0032, ce type de porte-clé permet de générer de nombreuses clés privées à partir d'un seul point de départ. Cette « graine », une valeur aléatoire de 128 bits qui peut se présenter sous la forme de 12 mots en anglais, permet de sauvegarder et de restaurer facilement l'ensemble de ses clés sans avoir besoin d'aucune autre information. Source : https://bitcoin.fr/quest-ce-quun-hd-wallet/

52 Ameyaw,P.D.;deVries, W.T. Toward Smart Land Management: Land Acquisition and the Associated Challenges in Ghana. A Look into a Blockchain Digital Land Registry for Prospects. Land 2021, 10, 239. https://doi.org/10.3390/land10030239

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