GOUVERNEMENT & DÉMOCRATIE

SEPTEMBRE 2022

WWW.BLOCKCHAINFORGOOD.FR

BLOCKCHAIN @POLYTECHNIQUE
bpifrance SERVIR L'AVENIR
Caisse des Dépôts GROUPE
INSTITUT Louis Bachelier
PB PositiveBlockchain.io

A PROPOS

BLOCKCHAIN FOR GOOD

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

NOS PARTENAIRES

BLOCKCHAIN @POLYTECHNIQUE

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

Caisse des Dépôts GROUPE

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

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

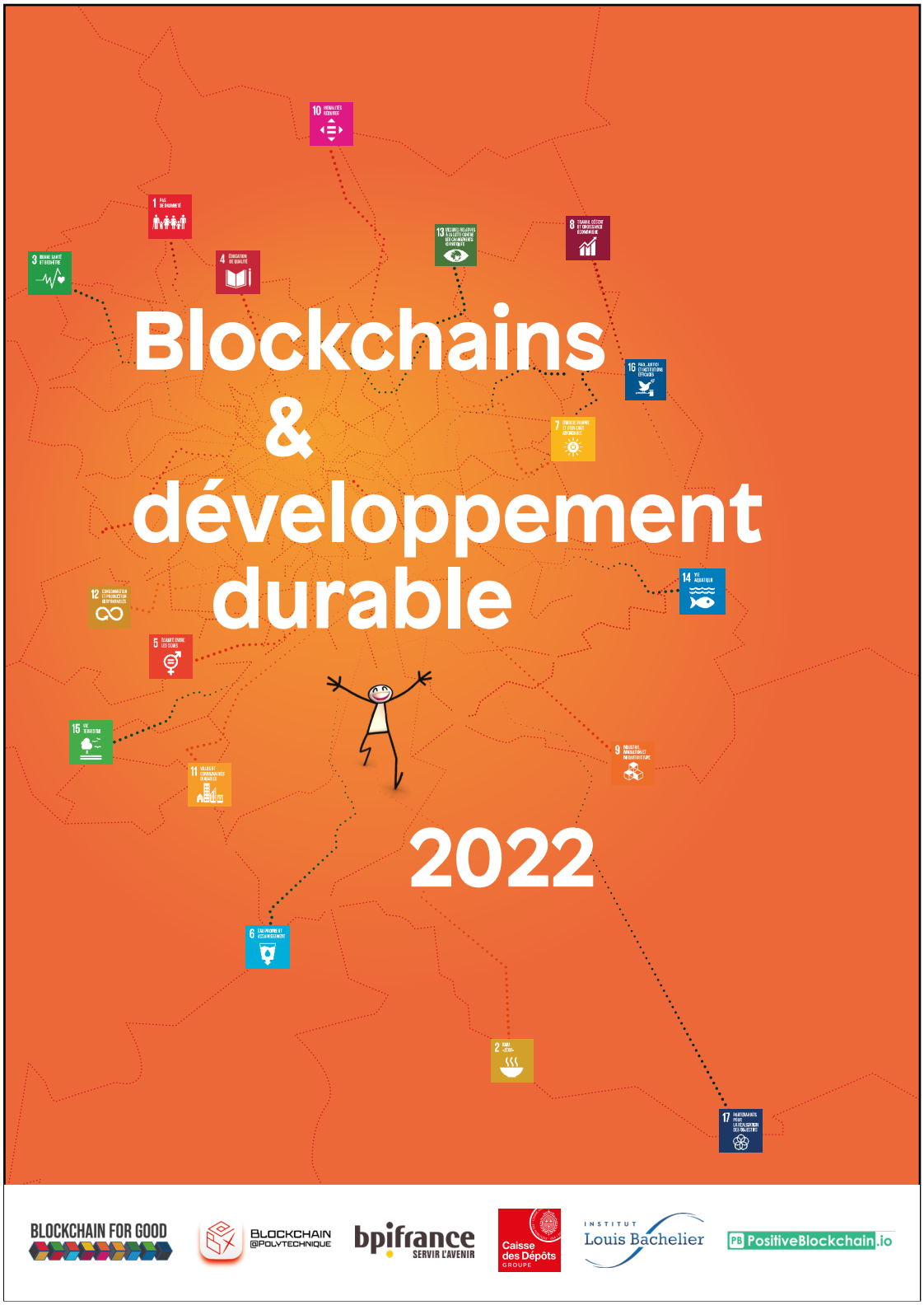
Bpifrance finance les entreprises - à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi leur activité export à travers une large gamme de produits. Conseil, université,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

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

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

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

CE CAHIER EST UN EXTRAIT DU RAPPORT :



LIBREMENT TELECHARGEABLE SUR BLOCKCHAINFORGOOD.FR

AUTEURS

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

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

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

CONTRIBUTEURS

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

RELECTEURS - CAHIER DÉMOCRATIE ET GOUVERNEMENT

Noémie Dié, Jacques-André Fines Schlumberger, Audran Gouis.

TABLE DES MATIÈRES

GOUVERNEMENT ET DÉMOCRATIE

par **Pierre Noro**, enseignant « *Blockchain for Public Good, Governance and Regulation* » à Sciences Po Paris, Directeur des opérations de Pebble.

Nombre de projets dans la base : 78

Nombre de projets actifs : 34

Nom des projets actifs : Aragon ; Bitland ; Blockademia ; Callisto ; Chromaway ; Civic Ledger ; DAOhaus ; DAOstack ; Democracy Earth ; District0x ; EBSI ; Electis ; FlexFinTx ; Followmyvote ; Geon Network ; Gitcoin ; GivEth ; Gmerits ; Horizen ; Horizon State ; Originalmy ; OS City ; Polys ; Possible Today Foundation ; Procivis ; Singapore Smart Nation Initiative ; Smart Certificate ; Smart Dubai ; SourceCred ; Tellor ; The Bounties Network ; The Commons Stack ; TruBudget ; Voatz ; *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/

Comment une technologie résolument anarchiste, libertarienne, dans un sens « anti-État » peut désormais être présentée comme une opportunité pour la rénovation de nos systèmes démocratiques et des administrations publiques, au niveau local, national et international ?

Il existe une porosité surprenante, un dialogue étonnant entre les écosystèmes blockchain et les institutions publiques. Les réponses apportées par l'une, face aux failles systémiques et aux abus des tiers de confiance, sont désormais une source d'inspiration essentielle pour l'innovation publique.

Les technologies blockchains en général, les systèmes de gouvernance décentralisés en particulier, remettent en question la place de la confiance dans l'organisation de nos sociétés.

Loin du fantasme d'être des systèmes « *trustless* », qui se structurent uniquement par le biais d'une mathématique de règles de marché, l'utilisation des registres décentralisés et de mécanismes d'incitation à la participation au réseau interrogent les conditions de la confiance dans une gouvernance plus horizontale et polycentrique[1].

1 Primavera de Filippi, Morshed Mannan, Wessel Reijers. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, Elsevier, 2020, https://hal.archives-ouvertes.fr/hal-03098449

Alors qu'un nombre grandissant d'États, pourtant pourvus d'une longue tradition républicaine et démocratique, voient arriver à leurs têtes des leaders élus sur des programmes politiques à tendance populiste et illibérale, et que les sondages internationaux signalent une crise globale et profonde de l'attachement des populations à la démocratie, les expérimentations présentées ici, qu'elles aient été vectrices d'un véritable impact social positif ou bien qu'elles soient restées au stade de projet, nous livrent des leçons précieuses sur les conditions essentielles de succès pour des mécanismes de gouvernance démocratiques : l'ouverture et la transparence.

Bitcoin, une idéologie et une gouvernance alternative

En inscrivant dans le « *genesis block* », le tout premier bloc de la blockchain Bitcoin, une référence à la une du journal *The Times* paru le 3 janvier 2009, Satoshi Nakamoto ne fait pas que poser la fondation de sa création. Il revendique explicitement, dès les origines de Bitcoin, son caractère révolutionnaire, alternatif, voire anarchiste.

> « *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*[2]. »

En un bref message, Satoshi Nakamoto réaffirme l'idéologie des cypherpunks[3] et la nécessité de s'affranchir d'un système financier et monétaire marqué par une crise profonde. Aux yeux de la petite communauté qui se fédère autour de Bitcoin et des précédentes expérimentations qui ont mené au premier crypto-actif d'envergure, les États et leur pouvoir centralisateur sont tout aussi coupables que les établissements financiers à l'origine de la crise de 2008.

Les « *bailouts*[4] » réalisés à grands renforts d'argent public sont à la fois des exemples du caractère arbitraire des monnaies souveraines et des symptômes d'un système monétaire insuffisamment transparent, ouvert et décentralisé.

Les technologies blockchains rendent possibles des alternatives aux monnaies souveraines, mais aussi aux organisations centralisées, qu'elles relèvent du secteur privé ou qu'elles soient d'origine étatique. Bitcoin prouve rapidement qu'un registre distribué au sein d'un réseau de pair-à-pair, ouvert, *open source* peut devenir une infrastructure numérique publique permettant à ses utilisateurs pseudonymes d'enregistrer et de partager de manière synchronisée et sécurisée des informations identiques et immuables, qu'elles soient financières ou non.

2 «The Times 03/Jan/2009 La chancelière au bord d'un second plan de sauvetage des banques ».
3 Mot valise construit à partir de « *cipher* », chiffrement et « *punk* ». Il désigne les personnes qui préconisent l'utilisation généralisée de la cryptographie forte et des technologies de renforcement de la vie privée comme une voie vers le changement social et politique.
4 « Renflouement », l'octroi d'une aide financière à une société ou à un pays afin de lui éviter la faillite ou la

Les technologies blockchains ne remettent pas seulement en cause le monopole de l'État sur la monnaie souveraine : elles questionnent le rôle de tout tiers de confiance, de tout intermédiaire et de toute organisation centralisée et verticale.

Ces valeurs d'ouverture, de transparence et d'horizontalité au cœur de Bitcoin se retrouvent également dans sa gouvernance. Le programme qui permet à n'importe qui d'accéder au registre et d'en devenir validateur est *open source* (voir Introduction). La gouvernance du réseau est d'abord informelle, la communauté s'organise autour de forums et de boucles emails avant que plusieurs *core developers* (Amir Taaki, Luke Dashjr et Pieter Wuille notamment) standardisent le système de Bitcoin Improvement Proposals[5] (BIP), durant l'été 2011.

Reprenant les outils de collaboration mis en place dans d'autres communautés *open source*, les *Bitcoin Improvement Proposals* deviennent le format permettant à n'importe qui de proposer une mise à jour du code de Bitcoin. Une fois présentés à la communauté, toujours *via* la *mailing list* ouverte Bitcoin, et discutés une première fois pour s'assurer de leur pertinence, les BIPs sont soumis aux votes des mineurs[6], qui signalent dans chaque bloc validé leur soutien à un ou plusieurs BIPs. Le pouvoir de vote est réparti proportionnellement à la puissance de calcul de chaque mineur, puisque la probabilité de voir son vote pris en compte est la même que celle de produire le prochain bloc valide.

Si pendant une certaine période, plus de 75 % ou 95 % des blocs contiennent un signal favorable, le BIP concerné est implémenté. La blockchain Bitcoin opère donc non seulement comme une infrastructure permettant la génération et les échanges de son propre crypto-actif, le Bitcoin, mais également en tant qu'outil intégré de vote et de coordination pour soutenir sa propre gouvernance.

Néanmoins, ce modèle de gouvernance impliquant, d'un côté, la communauté Bitcoin dans son ensemble et, d'autre part, les mineurs, a montré plusieurs limites. Malgré son caractère ouvert, participatif et transparent, la gouvernance de Bitcoin se revendique plus d'une forme de méritocratie que de démocratie : les discussions informelles qui amènent à la soumission des BIPs dans la communauté, quoique ouverte à tous, confèrent un rôle majeur aux groupes de *core developers* les plus actifs et les plus influents. Plus important encore, l'adoption de certains BIPs jugés essentiels à l'évolution

banqueroute.

5 Bitcoin Improvement Proposals : un document conçu pour proposer et introduire des fonctionnalités ou des informations aux utilisateurs de l'infrastructure Bitcoin.

6 Dire que les mineurs « votent » est, comme l'explique Peter Wuille, une simplification : les mineurs ne votent pas mais signalent leur soutien à des BIP qu'ils sont prêts à mettre en place. Tout utilisateur de Bitcoin opérant un *full node* peut installer une version du programme implémentant n'importe quelle mise à jour qu'il pense pertinente, au risque que son programme ne puisse plus reconnaître les blocs validés par des mineurs opérant une version non-compatible de Bitcoin.

technique de Bitcoin sur le long terme par la communauté se heurte parfois aux objectifs économiques de maximisation des profits liés à l'activité des mineurs.

Cette divergence s'est par exemple faite ressentir à l'été 2017 autour des différents BIPs visant à apporter plus de scalabilité[7] pour Bitcoin. Face à une communauté réclamant la mise en œuvre de ces mises à jour pour désengorger le réseau et augmenter sa capacité, certaines « *pools* de mineurs »* redoutant, entre autres, la perte d'une partie de leurs revenus[8] ont considérablement ralenti l'adoption des BIPs concernés.

Les divergences entre les *core developer* et les mineurs autour des enjeux de scalabilité sur Bitcoin sont d'ailleurs à l'origine de nombreux *hard forks** donnant naissance à une myriade de *altcoins** ré-utilisant le code et l'historique de Bitcoin, tout en implémentant des modifications à son code source.

Le caractère *open source* des technologies blockchains autorise en effet n'importe quel utilisateur soutenant une proposition minoritaire sur un protocole de créer sa propre version transformée d'une blockchain existante. Puisque l'historique d'une blockchain source est répétée dans la nouvelle au moment du *hard fork**, tout utilisateur ayant des actifs associés à ses adresses avant le schisme détient également des actifs dans la nouvelle blockchain.

C'est alors à la communauté de jouer le rôle d'arbitre en choisissant d'utiliser une blockchain, l'autre ou bien même les deux.

Les premiers usages : les blockchains comme substituts aux tiers de confiance

Alors que Bitcoin démontre rapidement sa capacité à servir de registre décentralisé, sécurisé et immuable pour de l'information financière et extra-financière, de nombreuses expérimentations pionnières visent à utiliser cette capacité pour «notarier» des documents dès les années 2010. Des entrepreneurs développent des projets et des standards où une blockchain est utilisée pour ancrer des preuves d'existence numériques uniques de documents concernant des propriétés foncières, des preuves d'identité, des certificats et des diplômes. (Voir notamment les Chapitres « Identité et propriété » et « Éducation et emploi »).

Ces cas d'usage proposent donc de substituer des registres décentralisés et ouverts aux tiers de confiance traditionnels. Exit l'État, les autorités et institutions publiques ou bien les intermédiaires privés chargés de rassembler en un seul endroit et de manière standardisée l'information générée par tout un écosystème d'acteurs pour ensuite agir comme les uniques dépositaires de l'information certifiée.

7 Vient de l'anglais « *scale* » qui signifie « échelle ». Désigne la capacité d'un produit ou service informatique à s'adapter aux fluctuations de la demande en conservant ses différentes fonctionnalités.
8 Certains mineurs, au moins à court terme, semblaient estimer bénéficier davantage de l'augmentation des frais de transactions causés par la saturation des blocs.

L'utilisation d'une blockchain permet d'ancrer des preuves cryptographiques accessibles à tous qui permettent de vérifier l'authenticité d'une déclaration ou d'un document en la possession du vérificateur, garantissant l'identité du certificateur et son horodatage.

Ces nouveaux cas d'usage ont été, dans un premier temps, explorés par des utilisateurs animés par les mêmes idéologies libertarienne ou crypto-anarchistes au cœur de Bitcoin.

Ils visent logiquement des secteurs où la confiance est faible et l'acquisition de l'information coûteuse : des environnements complexes impliquant un très grand nombre d'acteurs (suivi de chaîne logistique, commerce international, traçabilité des biens…), des tiers de confiance techniquement défaillants, frauduleux ou bien situés dans des juridictions marquées par l'instabilité politique, par un pouvoir autoritaire, illibéral et/ou un haut niveau de corruption (comme Bitland au Ghana et au Honduras ou encore BenBen au Ghana - Voir Chapitre Identité et propriété), mais aussi des marchés peu liquides où les intermédiaires profitent de leur rente informationnelle pour ériger des barrières à l'accès d'informations essentielles (par exemple le marché de la propriété intellectuelle, identité numérique…).

Les blockchains au service des tiers de confiance

Pourtant, ce sont les expérimentations portées par des tiers de confiance historiques, notamment des institutions publiques, qui permettent à ces cas d'usage de gagner en visibilité aux yeux du grand public. Ce n'est un paradoxe qu'en apparence. Pour les institutions capables de surpasser la crainte initiale induite par l'idéologie au cœur de Bitcoin et de s'entourer des compétences requises pour développer des projets pilotes, les technologies blockchains représentent une aubaine pour montrer leur capacité à innover et moderniser des processus parfois peu ou pas digitalisés.

D'autant que si une blockchain permet de garantir l'existence des preuves cryptographiques d'informations et de leurs auteurs, elle reste un système « *garbage in, garbage out*[9] » : elle ne suffit pas à elle seule à garantir la validité des informations ancrées.

Loin de signifier la fin de tous les intermédiaires, les technologies blockchains ont donc un besoin essentiel de tiers de confiance pour importer des informations authentiques qui sont extérieures aux données générées *on-chain**.

Avec des responsabilités similaires aux *oracles**, les tiers de confiance peuvent profiter des technologies blockchains

9 Le biais des données, ou GIGO (*Gargage In, Garbage Out*), consiste en la prise en compte d'informations erronées ou de biais cognitifs potentiels – aussi cohérent ou utile puisse-t-elle paraître – et qui donnera des résultats inexacts.

pour procéder à l'enregistrement de données dont ils garantissent, en signant les ancrages, l'origine, mettant en jeu leur propre réputation afin de générer de la confiance autour des données certifiées.
Les expérimentations visant à utiliser une blockchain comme une infrastructure transparente, immuable et sécurisée pour l'enregistrement et la consultation de données publiques sont extrêmement nombreuses et varient en complexité. L'État de Genève avait, en 2017, utilisé Ethereum pour émettre des certificats permettant de vérifier des extraits de son registre du commerce[10].

En Mars 2018, la Comisión Nacional de Energía chilienne lance son portail « Energia Abierta » (Énergie Ouverte) et utilise également Ethereum pour ancrer les données publiques qui y sont publiées[11]. La même année, plusieurs collectivités territoriales indiennes, notamment dans le Bengale-Occidental, utilisent la blockchain pour sécuriser les certificats de naissance[12,13], et l'une des autorités locales de New Delhi considère d'emboîter le pas avec ses propres certificats de naissance et de décès cette année[14].

L'entreprise **OSCity**[15] est l'un des pionniers de la modernisation des services publics en Amérique Centrale et du Sud. En partenariat avec Unicef Innovate et l'Open Government Partnership, l'entreprise mexicaine a collaboré à la mise en place de systèmes expérimentaux utilisant la blockchain pour moderniser l'action publique de gouvernements locaux en Argentine (certification des résultats de la loterie publique dans la province du Rio Negro, financements publics pour la culture dans la municipalité de Bahía Blanca), au Costa Rica (attribution des licences de distribution d'alcool dans les localités de Quepos et de Grecia), au Brésil (certification des données des transports publics de la ville de Teresina) et au Mexique (certification des licences numériques de distribution d'alcool et de permis de construire dans la municipalité de San Nicolás).
Forte de cette expérience, l'entreprise travaille désormais à l'intégration d'une plateforme basée sur Ethereum articulant identité numérique, émission de certificats et outils de *smart city.*

10 « Rapport d'expérimentation Blockchain », Ville de Genève, consulté le 6 juillet 2022, https://www.ge.ch/document/rapport-experimentation-blockchain
11« Blockchain as an Information System in Chile: The Case of Open Energy Project - Chilean's Ministry of Energy », Stefania Pareti, Ignacia Núñez, Revista Ibérica de Sistemas e Tecnologias de Informação; Lousada N° E39, (Jan 2021): 554-568.
12 « A 1st in Bengal, baby gets blockchained birth certificate », Udit Prasanna Mukherji, Suman Chakraborti, Times of India, December 20, 2018, http://timesofindia.indiatimes.com/articleshow/67170551.cms
13 « Indian State Government Will Issue Birth Certificates on a Blockchain», CCN, October 2, 2020, https://www.ccn.com/indian-state-government-will-issue-birth-certificates-on-a-blockchain/
14Computer No. : 65981 Information technology department New Delhi municipal council, Palika Kendra: new delhi no. d-dfa/ January 25, 2021, https://www.medianama.com/wp-content/uploads/2021/06/New-Delhi-Blockchain.pdf
15 « About », OS City, retrieved July 6, 2022, https://www.os.city/

Ces cas d'usage ont prouvé que les tiers de confiance, en particulier les autorités publiques, peuvent utiliser les technologies blockchains afin de garantir un accès plus sécurisé et transparent à des données publiques et de faciliter l'émission et la vérification de documents officiels.

Puisque ces expérimentations permettent de limiter les risques des fraudes, de faciliter certaines démarches administratives et d'apporter plus de transparence dans l'action publique, luttant de ce fait contre la corruption, elles contribuent à la poursuite des objectifs de développement durables établis par l'ONU, en particulier les objectifs 11 – Villes et communautés durables et 16 – Paix, justice et institutions efficaces[16].

Bien qu'ils reposent sur une utilisation finalement assez simple des technologies blockchains, l'utilisation de tels registres pour stocker des données publiques est toujours d'actualité, comme le montre l'annonce à l'été 2021 par l'État de Quintana Roo, au Mexique, de la signature d'un accord de collaboration entre la *startup* GenoBank.io et l'Institut public d'Innovation et de Technologie de Quintana Roo pour certifier l'authenticité des résultats des tests COVID, dont 20 % seraient falsifiés au niveau national selon le COMED (Conseil Mexicain des Entreprises de Diagnostic médical)[17]. Ce projet, conçu en réaction à un scandale sanitaire causé par l'infection de plusieurs étudiants argentins en échange dans l'État mexicain après avoir été testés négatif dans un laboratoire exerçant sans autorisation officielle, promet une vérification simple et rapide, y compris à l'international, respectueuse des données personnelles des utilisateurs.

Néanmoins, le développement de cet outil, prévu pour être déployé sur la blockchain Avalanche[18], pourrait bien être rattrapé par les limites d'un autre projet porté par le congrès du Quintana Roo. En effet, le parlement local a décidé de ne pas renouveler son partenariat avec cette blockchain de « troisième génération » concernant l'archivage sur Avalanche des documents législatifs, après sept mois d'utilisation[19].

Le contrat à 600 000 pesos mexicains (près de 26 000 euros) signé par la précédente législature a été jugé trop coûteux pour la nouvelle, ne voyant pas l'intérêt de financer un outil « *surqualifié pour les besoins du pouvoir législatif*[20] *»*,

16 On peut également ajouter, de manière plus secondaire, les Objectifs de développement durable 10 – Inégalités réduites et 17 – Partenariats pour la réalisation des Objectifs.
17 « Quintana Roo detectará pruebas falsas de Covid-19 con blockchain de Avalanche », Cancunissimo, 8 juillet 2021, https://cancunissimo.mx/quintana-roo-detectara-pruebas-falsas-de-covid-19-con-blockchain-de-avalanche/
18 « Welcome to Multi-Verse », Avalanche, retrieved July 6, 2022, https://www.avax.network/
19 « Retiró congreso local sistema de blockchain por ser sobrecalificado para sus necesidades », Iriamna Caceres, QuintaFuerza, 11 octobre 2021, https://quintafuerza.mx/quintana-roo/cancun/retiro-congreso-local-sistema-de-blockchain-por-ser-sobrecalificado-para-sus-necesidades
20 « Mexico fights black market for covid tests with avalanche blockchain », Quintana Roo, June 8, 2021, https://qroo.gob.mx/iqit/mexico-fights-black-market-covid-tests-avalanche-blockchain

le système informatique du congrès permettant déjà un accès ouvert à toutes les données publiques, quoique sans ancrage cryptographique dans une blockchain.

L'exemple de Quintana Roo est symptomatique des limites de cette « première vague » d'expérimentations visant à moderniser les missions des tiers de confiance en utilisant des technologies blockchains pour mieux certifier des informations publiques.

En premier lieu, le manque de moyens et de volonté politique amènent souvent ces expérimentations à rester au stade de prototype. Même lorsqu'elles valident la faisabilité technique, elles sont rarement déployées par des institutions et/ou à destination des publics qui en ont le plus besoin (voir encadré).

De plus, nombreuses sont les expérimentations qui, réalisées au sein d'une seule entité chargée de l'enregistrement d'un seul type de données publiques - parfois ne représentant même pas un risque sérieux de fraude, de manque de transparence ou de déficit d'accès - pour une aire géographique et une population-cible restreinte, ont reproduit des structures de données organisées en silo, verticales et peu pratiques à l'usage. Leur valeur ajoutée est par conséquent parfois marginale, d'autant qu'elle peut se heurter à l'augmentation des frais des transactions liés à l'utilisation d'une blockchain publique, surtout si elle a recours au mécanisme de consensus de la *Proof-of-Work**, comme c'est le cas d'Ethereum.

Côté utilisateurs, le manque d'interopérabilité ou de standardisation entre les services peut rendre l'utilisation des blockchains pour vérifier les informations certifiées laborieuses, au point d'en devenir rédhibitoire.

Pour illustrer ce point, en l'absence d'un vérificateur commun permettant de contrôler les certificats numériques de tests Covid de tous les citoyens mexicains, difficile d'imaginer qu'un utilisateur hors de l'État du Quintana Roo, sans même parler d'un garde-frontière argentin, fasse vraiment l'effort d'accéder à la preuve ancrée sur une blockchain publique pour s'assurer que le QR code présenté par un citoyen de cet État est bel et bien valide.

Si la facilité d'usage n'est pas au rendez-vous, l'utilisateur risque de préférer d'ignorer la preuve apportée par une blockchain et de revenir au processus qui lui est le plus familier : faire confiance au tiers.

Utiliser des blockchains pour sécuriser l'accès ouvert aux données publiques : un dilemme d'innovation publique

La preuve d'antériorité ne fait pas valeur de preuve

En matière financière, l'information que contient une blockchain publique se suffit à elle-même pour générer la confiance nécessaire aux interactions entre les utilisateurs de son crypto-actif. Pour des informations « extérieures » à la blockchain, l'inscription dans un registre décentralisé peut permettre d'établir une preuve d'antériorité, les propriétés cryptographiques d'une blockchain permettant au détenteur d'une information de prouver sa connaissance de l'information à un moment donné, en signant une transaction contenant l'information (ou une référence à celle-ci) qui est ensuite intégrée à un bloc validé à un moment donné.

Cependant, selon le principe du « *garbage in, garbage out* » (déchet en entrée = déchet en sortie), la validité de cette information n'est pas intrinsèquement certifiée par le système, qui ne peut que vérifier la validité mathématique de la transaction. Les tiers de confiance offrent, en plus de l'enregistrement public, une valeur ajoutée supplémentaire, la valeur de preuve, reconnue par la communauté. Par exemple, la valeur de preuve d'un acte notarié ne provient pas seulement de l'autorité conférée par le statut d'officier public du notaire, mais aussi par sa mission de s'assurer de la bonne procédure, de la forme authentique de l'information et du consentement éclairé des parties prenantes à un acte.

Cependant, un tiers de confiance défaillant ou frauduleux pourrait enregistrer des informations erronées dans le registre. A condition qu'elle soit publique, l'utilisation d'une blockchain rend cette information publiquement visible, ce qui peut favoriser les recours de la victime d'une erreur ou d'une entrée frauduleuse, mais elle ne résout pas, à elle seule, le problème de la confiance envers les institutions.

Effet de réseau et masse critique

Un autre facteur déterminant pour qu'un service public fondé sur une blockchain puisse générer un niveau de confiance et d'autorité suffisante est l'effet de réseau. Plus le recours à un outil d'enregistrement de l'information est répandu dans une communauté, plus la réputation de l'information enregistrée et accessible via cet outil est forte.

La difficulté pour les projets à dépasser le stade du pilote et à être généralisés, par manque de ressources ou parce qu'un déploiement local ne permet pas de valider la valeur ajoutée, peut les empêcher d'atteindre une masse critique de données et d'utilisateurs nécessaire à leur succès.

Asymétrie des besoins et de l'accessibilité

Il en résulte que les services publics fondés sur des blockchains sont rarement compétitifs face aux services publics traditionnels qui bénéficient, dans les pays développés et avec des institutions libérales, d'un fort effet de réseau pour leur juridiction et d'une certaine capacité à générer de la confiance. En revanche, ces services innovants peuvent être une alternative crédible dans des pays touchés par de hauts niveaux de corruption, dont les institutions sont systématiquement défaillantes, où les systèmes d'information de l'administration sont précaires, ou encore pour les communautés ne s'inscrivant pas facilement dans une juridiction précise (personnes migrantes et réfugiées, communautés transnationales…).
Ironiquement, ces populations pour lesquelles les services publics fondés sur une blockchain sont les plus attrayants sont souvent des communautés avec le moins de ressources pour les mettre en œuvre. Les bénéficiaires qui gagneraient le plus à avoir recours à ces services sont également ceux pour lesquels les barrières à l'entrée sont les plus nombreuses et importantes.

Les blockchains pour construire des Nations sans État

Afin de dépasser ce problème des données organisées en silo et tirer véritablement profit de la structure décentralisée des technologies blockchains et de leurs protocoles de consensus, plusieurs projets ont envisagé des approches beaucoup plus transverses, avec l'ambition de construire toute une administration numérique publique fondée sur des technologies blockchains. Comme pour les services de certification, les initiatives officielles furent précédées par des projets beaucoup plus radicaux, pétris d'idéaux anarchistes ou libertariens, ayant pour idéal de construire des alternatives aux États tels que nous les connaissons.

Nombreux sont les projets de micro-nations à avoir revendiqué vouloir utiliser une blockchain publique comme infrastructure numérique de leurs révolutionnaires administrations ouvertes. Que ce soit l'adoption du Bitcoin comme monnaie officielle de la non-officielle principauté de Pontinha, le projet de création du Merit, le crypto-actif propre au Liberland, micro-nation nichée sur les rives du Danube, entre la Serbie et la Croatie, qui devait également utiliser une blockchain pour son système d'arbitrage juridique, ou les concepts d'utopies crypto-libertariennes (la nation vogante Entropy, le Floating Island Project en Polynésie, FreeSociety[21], le projet de

21 « A floating Pacific island is in the works with its own government, cryptocurrency and 300 houses », Camille Bianchi, May 18, 2018, https://www.cnbc.com/2018/05/18/floating-island-is-planned-with-government-cryptocurrency-and-houses.html

Puertopia[22], aussi appelé Sol, à Puerto Rico...), aucune de ces expérimentations ou propositions n'a égalé, en termes de visibilité, Bitnation.

Prolongeant les concepts au cœur de l'idéologie crypto-anarchiste, **Bitnation**[23] est fondé le 14 juillet 2014 par Susanne Tarkowski Tempelhof pour mettre en place un « *système de gouvernance en pair-à-pair*[24] » à travers lequel n'importe quel utilisateur peut devenir membre d'une communauté de citoyens virtuels sans territoire ni État.

Cette vision à la fois nourrie par l'histoire personnelle de sa fondatrice (fille d'une mère Française et d'un père Polonais vivant en Suède, elle a travaillé pendant plusieurs années dans des zones de guerre où les États-nations se sont écroulés, en Afghanistan et en Libye[25]) et par les valeurs de Bitcoin, est rendue possible par l'émergence de la blockchain Ethereum et des premières Organisations autonomes décentralisées (DAO*).

C'est avec un ensemble de *smart-contracts** déployés sur cette blockchain d'un genre nouveau que Bitnation promet une variété de services à quiconque veut rejoindre la première « *nation volontaire, décentralisée et sans-frontière*[26] ».

Les premiers services de « Gouvernance DIY[27] » offerts aux utilisateurs sont un outil d'identité numérique, le « Digital ID », et, logiquement, un service de notariat public leur permettant d'enregistrer des certificats de naissance, de mariage, titres de propriété et autres documents importants sur la blockchain Ethereum.

Outre les pionniers de la communauté crypto et les *digital nomads*[28] partageant la vision de la fondatrice du projet, Bitnation compte des *early adopters*[29] plus surprenants. A partir de l'automne 2015, le Bitnation Refugee Emergency Response propose en effet aux personnes migrantes et réfugiées d'obtenir un Blockchain Emergency ID ainsi qu'une carte de paiement en crypto-actifs et en monnaie fiat*, la Bitnation Bitcoin Visa Debit Card.

Ce dispositif a pour mission de faciliter leur accès aux services dans leur pays d'accueil, d'accélérer leur intégration et le rapprochement familial. Pour des personnes en situation de migration, parfois apatrides ou sans-papiers,

22 « Making a Crypto Utopia in Puerto Rico », Nellie Bowles, February 2, 2018, https://www.nytimes.com/2018/02/02/technology/cryptocurrency-puerto-rico.html
23 « Enter Pangea », Bitnation, retrieved July 6, 2022, https://tse.bitnation.co/
24 « Bitnation.co », Internet Archive, March 3, 2019, https://web.archive.org/web/20190303234601/https://tse.bitnation.co/
25 « La Blockchain au service des réfugiés », Audrey Bauer, Usbek&Rica, 11 août 2016, https://usbeketrica.com/fr/article/la-blockchain-au-service-des-refugies
26 Bitnation documents, retrieved July 7, 2022. https://tse.bitnation.co/documents/
27 DIY pour « *Do It Yourself* » et qui se traduit par « faites-le vous-même ».
28 Les « *digital nomads* » désigne des personnes qui adoptent un mode de vie dans lequel ils voyagent fréquemment tout en travaillant en même temps.
29 Désigne les individus les plus rapides à adopter une nouvelle technologie ou une innovation.

confrontés à des parcours administratifs longs et complexes, même une carte d'identité privée, sans valeur légale hors de sa « juridiction blockchain » mais infalsifiable, peut représenter un atout dans leur parcours d'intégration. Cette initiative sera d'ailleurs récompensée par le Grand Prix 2017 du Forum Netexplo, en partenariat avec l'UNESCO[30].

Mais cette reconnaissance par une branche de l'ONU n'est pas le premier contact officiel entre Bitnation et une organisation publique. En 2015, à peine un an après leurs créations mutuelles, le service de notariat sur la blockchain de Bitnation est également mis à disposition des participants au programme de e-Residency estonien. Même si l'utilisation du Bitnation Public Notary ne confère pas de valeur juridique aux documents dans la juridiction estonienne, ce partenariat permet à Bitnation d'intégrer la signature électronique estonienne pour les e-residents afin de légitimer son service et démontre la possibilité d'une collaboration entre une DAO* et un État souverain.

Grâce à ces coups d'éclat médiatiques, Bitnation, désormais immatriculé au Belize, a pu procéder, après un échec en 2014, à deux ICOs en 2017 puis en 2018, amassant plus de 30 millions de dollars[31]. Ce tour de table a permis de lancer « Pangea », décrite dans le livre blanc publié à l'occasion comme une suite d'outils décentralisés (*smart contracts** sur Ethereum, stockage IPFS* et utilisation d'un protocole de communication en pair-à-pair dérivé de Secure Scuttlebutt[32]) avec lesquels n'importe quel utilisateur ou groupe d'utilisateurs peut lancer sa propre Decentralized Borderless Voluntary Nation (DBVN), avec sa propre constitution, ses propres mécanismes de gouvernance, utilisant les services de Bitnation ou en proposant de nouveaux.

Pangea fonctionne aussi comme la strate fondamentale de ce réseau holocratique[33] de DBVN interopérables, opérant un mécanisme d'arbitrage en cas de litige dans l'exécution des services proposés ou des contrats entre les citoyens. Pangea est donc conçu pour intégrer un système de réputation algorithmique (dénommé Lucy AI) essentiel au fonctionnement de son processus « Jurisdiction as a Service », par lequel les utilisateurs ou les *smart-contracts** peuvent désigner, en cas de litige, des arbitres ayant démontré leur capacité à collaborer à travers les DBVN.

30 « The Netexplo Forum celebrated its 10th edition », UNESCO, May 5, 2020, https://en.unesco.org/news/netexplo-forum-celebrated-its-10th-edition
31 « Bitnation », ICOHolder, retrieved May 17, 2022, https://icoholder.com/fr/bitnation-3557
32 « Scuttlebutt », Scuttlebutt, retrieved July 6, 2022, https://scuttlebutt.nz/
33 L'holocratie (*holacracy* en Anglais), que Susanne Tarkowski Tempelhof revendique parmi ses inspirations est, selon l'Office québécois de la langue française un « mode de gouvernance qui recourt au principe d'intelligence collective et dont la structure, non hiérarchisée, se compose d'équipes reliées entre elles par des objectifs communs et détenant chacune la pleine autorité dans ses champs d'expertise. » Plus particulièrement, Bitnation défend un idéal d'holocratie constitutionnelle, où n'importe quel groupe d'individus peut se rassembler autour de valeurs et objectifs communs, adoptant une constitution pour organiser leur gouvernance interne.

Début 2018, Bitnation comptait plus de 12 000 citoyens répartis dans plus de 200 *voluntary nations*. Pourtant, depuis 2019, le code source, principalement composé de bribes de programmes disparates à l'état de preuve de concept, à l'exception d'outils de certification et d'émission de *tokens* déjà standards dans l'écosystème blockchain, n'est plus mis à jour[34].

Quelques rocambolesques déclarations d'anciens développeurs et contributeurs laissent à penser que le projet a toujours davantage reposé sur sa vision et sa communication que sur le développement de services décentralisés[35].

En l'absence de réelle mesure d'impact[36] et de code effectivement réutilisable, Bitnation était, selon toute vraisemblance, principalement un « *vaporware* », un produit fantôme, une nation sans état, sans frontière mais aussi sans code, sans réalité effective, comme les projets de micro nations déjà évoqués.

Il a néanmoins eu pour mérite de prouver que le concept d'organisations décentralisées permettant à des communautés transnationales de se gouverner par elles-mêmes sans État, grâce à un ensemble d'outils *open source* reposant sur des technologies de registre distribué répond, au moins en apparence, à des attentes réelles, inspirant de nombreuses autres projets[37], et qu'il n'est pas irréconciliable ni même incompatible avec celui des États souverains.

Fédération de services et interopérabilités des administrations sur des blockchains

Difficile d'estimer dans quelle mesure les exemples de Bitnation et des premières organisations autonomes décentralisées (DAO*) focalisées sur la gouvernance décentralisée ont pu influencer les institutions publiques dans différents pays. Toujours est-il que plusieurs États décident d'aller plus loin que la mise en œuvre d'expériences pilotes axées sur un cas d'usage unique, souvent celui de la certification de données et de documents publics (voir partie 3) pour annoncer des programmes de e-gouvernement fondés sur des technologies blockchains.

L'Estonie est souvent citée comme le pays de référence à cet égard. Le jeune État balte a profité de la relative absence d'administration publique suite à l'effondrement du bloc soviétique pour entreprendre la construction,

34 « Bitnation », Github, retrieved May 17, 2022, https://github.com/Bit-Nation
35 « The Perils of Radical Co-Creation », Tristan Roberts, Medium, March 24, 2018, https://aitheric.medium.com/the-perils-of-radical-co-creation-40fe2458281e
36 C'est-à-dire de données mesurant non seulement l'adoption générale d'une solution, mais également celles évaluant l'utilisation effective du projet et l'impact positif - ou négatif - ainsi généré sur la vie des utilisateurs. Dans le cadre de Bitnation, les chiffres parfois conséquents, comme les plus de 500 « Nations » et plus de 5 000 « contrats notarisés», sans plus de précision sur la nature de ces communautés, de ces contrats (exécutés ou non) et des actions qu'ils ont amenés, nous en apprennent finalement assez peu sur l'utilisation réelle de la plateforme faite par les utilisateurs. Ce problème est toutefois relativement courant vis-à-vis de ce genre de projet.
37 Citons notamment Nation3, CityDAO ou CatalanDAO.

peu après son indépendance en 1991, d'une infrastructure informatique ambitieuse pour ses institutions, conformément à sa stratégie *Tiigrihüpe* (« bond du tigre » en Estonien) visant à connecter et éduquer sa population aux nouvelles technologies numériques.

Les mises en production d'un réseau d'échange des données transverse pour toute l'administration (X-Road) en 2001, puis d'un système d'identité numérique dès 2002, puis de vote électronique pour les citoyens dès 2007 font de l'Estonie un pionnier du gouvernement numérique[38].

C'est en 2008, en réaction aux cyberattaques qui ont visé les sites gouvernementaux au printemps 2007 que l'Autorité des Systèmes d'Information estonienne (RIA) commence à travailler avec l'entreprise Guardtime pour tester sa solution de Keyless Signatures Infrastructure (KSI), officiellement lancée en 2012 au sein du ministère de la Justice, pour sécuriser le registre national des successions.

Le recours à la KSI, directement intégré à l'infrastructure X-Road est rapidement étendu aux ministères des Affaires Économiques et des Communications, au ministère de la Finance, au ministère de l'Intérieur et enfin à celui des Affaires Sociales. Il aura pour objectif de sécuriser les données judiciaires, de santé, des registres de propriété, d'entreprise ainsi que les informations du journal officiel estonien.

Cependant, il est important de noter que Guardtime a, dans un premier temps, fortement insisté pour que sa KSI ne soit pas confondue avec une blockchain. Sa technologie, antérieure même au lancement de Bitcoin, partage une structure de données faisant un usage similaire de la cryptographie. Elle permet, sur la base d'un *hash* de document, de générer une preuve d'existence, avec un *timestamp* mais aussi une signature permettant d'identifier l'auteur et l'émetteur de la requête.

Les *hashs** envoyés à la KSI sont organisés en arbres de Merkle* dont la racine est insérée dans une base de données à chaque seconde où les entrées sont liées entre elles par cryptographie, ce qui la rend immuable et non-réversible de la même manière qu'une blockchain[39]. En revanche, elle n'en partage pas le caractère décentralisé et ouvert permis par un protocole de consensus dit « de Nakamoto » puisque ce sont les serveurs « Aggregators », propriétés de Guardtime, qui forment les arbres de Merkle et assurent le consensus dans le réseau[40].

38 « KSI Blockchain in Estonia », Estonian Government, 2020, https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf
39 « Blockchain Designed for Supply Chains: Guardtime Supply Chain Framework », David Shorthouse, Michael Xie, Guardtime, April 2020, https://m.guardtime.com/files/Blockchain%20Designed%20for%20Supply%20Chains%20%282%29.pdf
40 « Guardtime KSI Definitions and Abbreviations », Guardtime, April 2021, https://m.guardtime.com/files/GT-KSI-DEF-v1.2-1.pdf

C'est d'ailleurs ce caractère permissionné (voire privé puisque le consensus est centralisé au sein d'une même organisation) de la KSI qui permet à Guardtime de traiter rapidement la quantité de données générées par les services publics estoniens compatibles, sans connaître les problèmes de scalabilité des blockchains publiques.

En plus de cette différence majeure, Guardtime n'a sûrement pas voulu associer son image à la sulfureuse réputation de Bitcoin et de premiers crypto-actifs[41]. Ce n'est qu'à partir de 2015 que Guardtime a décidé de surfer sur l'engouement nouveau autour des technologies blockchains. A la faveur d'un changement de communication à 180 degrés, l'entreprise a commencé à revendiquer l'infrastructure KSI comme une blockchain, même si la question de la pertinence technique de cette qualification fait débat, y compris au sein des autorités publiques estoniennes[42].

La stratégie de e-gouvernement estonienne a fortement influencé d'autres pays voulant moderniser radicalement les systèmes d'information qui sous-tendent les activités du secteur public. C'est le cas notamment de l'émirat de Dubai, dont la Dubai Blockchain Strategy présentée en octobre 2016 promettait de faire de Dubai « *la ville la plus heureuse du monde*[43] ». Centrée sur trois piliers –l'efficience de l'action publique, la création d'un écosystème et l'essor d'un *leadership* international en matière de blockchain – cette stratégie doit permettre de réaliser pas moins de 5,5 milliards de dirhams d'économie par an (plus de 1,3 milliards d'euros), soit l'équivalent du coût de construction du Burj Khalifa, la construction la plus haute du monde, l'un des emblèmes de la ville.

L'approche « *blockchain-first* » présentée par Mohammed bin Rashid Al Maktoum, émir de Dubai, est simple : en 2020, l'intégralité des services publics pertinents devront avoir effectué leur migration en passant du papier à des DLT. L'émirat a rapidement annoncé la mise en place d'une collaboration avec Consensys, IBM ainsi que Du, l'opérateur de télécommunications détenu par les Émirats arabes unis, pour créer le « *Blockchain Platform as a Service* » (désormais intégré à Dubai Pulse, une initiative conjointe entre Du et Smart Dubai) qui permet aux agences gouvernementales et institutions publiques de lancer de nouveaux services ou de porter les processus existants sur des blockchains permissionnées reposant au choix sur les technologies Ethereum ou Hyperledger Fabric.

41 Guardtime s'est même démarqué par un certain scepticisme envers les DLTs en général. « Guardtime », web.archive, retrieved July 21, 2022, https://web.archive.org/web/20190831005934/https:/guardtime.com/technology

42 « There is no blockchain technology in X-Road », Petteri Kivimäki, Nordic Institute for Interoperability Solutions, April 26, 2018, https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-roade.com/document/d/1I4BS2zBSODEFrsoKiTUymxjQsfl5tJFB/edit#

43 « Dubai Blockchain Strategy », Digital Dubai, retrieved July 21, 2022, https://www.digitaldubai.ae/initiatives/blockchain

Pas moins de vingt-quatre cas d'usage sont en cours d'exploration au sein des différentes institutions publiques de Dubai, parfois sous la forme de partenariats publics-privés, suivant un ensemble d'orientations, de règles et de bonnes pratiques présentées dans la *Dubai Blockchain Policy* publiée en 2019. Ils se répartissent dans huit industries : la finance, l'éducation, l'immobilier, le tourisme, le commerce, la santé, les transports publics et la sécurité[44].

On y retrouve quelques applications basiques, comme l'émission de certificats par les universités publiques, l'enregistrement des licences des praticiens spécialistes par l'Autorité de la Santé, un système de cadastre et d'hypothèques, un registre des entreprises, une « Cheque Chain » qui permet le suivi des chèques émis par la EmiratesNBD à l'aide de QR codes uniques[45]. D'autres projets se distinguent néanmoins en explorant des sujets d'application plus novateurs.

La « Dubai Vehicle Chain » est un projet de service de « *carnet de santé du véhicule* »[46] porté par la Roads and Transports Authority, ayant pour mission de créer un registre où toutes les parties prenantes du secteur de l'automobile pourraient maintenir un dossier d'information fiable et partagé, enregistrant tous les événements importants du cycle de vie de chaque véhicule dans le pays (achat, propriétaires successifs, cession, maintenance, accidents…).

Le Dubai Immigration Department testerait un registre des entrées et sorties du territoire de tous les visiteurs[47]. Le système Dubai Pay, qui permet déjà aux résidents et visiteurs de payer pour l'accès à certains des *smart services* et qui est utilisé par une cinquantaine d'entités publiques ou privées, a également migré son système de recouvrement et de remboursement sur une blockchain, passant d'une moyenne de quarante-cinq jours de traitement par dossier à deux semaines, avec dans certains cas un suivi des résolutions en temps-réel[48].

Cet effort de modernisation rapide, conjugué à d'autres initiatives de modernisation de l'action publique (Dubai10X, Smart Dubai 2021, Dubai

44 « Smart Dubai turns 5 ! », Digital Dubai, Comprehensive Booklet, January 2021, https://www.digitaldubai.ae/docs/default-source/publications/sd_anniversary_booklet_5years_en.pdf ?sfvrsn=818d909b_6
45 « Emirates NBD leads banking sector in cheque security by successfully rolling out 'Cheque Chain' at scale », Emirates NBD, April 15, 2018, https://www.emiratesnbd.com/en/media-centre/media-centre-info/ ?mcid_en=598
46Blockchain in the UAE government, United Arab Emirates, retrieved July 6, 2022, https://u.ae/en/about-the-uae/digital-uae/blockchain-in-the-uae-government
47 « Govchain », UAE, retrieved Jul 8 2022, https://govchain.world/uae/
48 « Emirates Blockchain Strategy 2021 », GovChain, retrieved May 17, 2022, https://govchain.world/uae/ ; Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates », United Arab Emirates Center for the Fourth Industrial Revolution, World Economic Forum, January 2020, https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_Case_Studies_and_Learnings_from_the_United_Emirates.pdf

Paperless Strategy…), est porté par toute l'administration, au niveau local, sous le pilotage de la Dubai Future Foundation et du Digital Dubai Office. Il s'articule également, au niveau fédéral, avec la « Emirates Blockchain Strategy », dévoilée en 2018 toujours par Mohammed bin Rashid Al Maktoum, vice-président et Premier-Ministre des Émirats Arabes Unis.

Cette stratégie est similaire à celle mise en œuvre à Dubai, puisqu'elle a pour but de surfer sur le même élan et de réemployer les mêmes technologies. Elle repose sur quatre piliers : le bonheur des citoyens et résidents, l'efficacité au sein du gouvernement, l'adoption d'une législation en avance de phase et la facilitation de l'entrepreneuriat global.

Son objectif n'est qu'à peine moins ambitieux que la feuille de route pour Dubai : 50% de toutes les transactions et échanges d'information effectués au sein de l'administration devront être enregistrées sur la blockchain en 2021, pour une économie chiffrée à 11 milliards de dirhams (près de 2,65 milliards d'euros), 77 millions d'heures de travail et presque 400 millions de documents qui n'auront plus besoin d'être imprimés.

Outre les solutions élaborées dans le cadre de Smart Dubai et déployées au niveau national (comme par exemple Abu Dhabi Pay, lancé en mai 2020[49]), la Emirates Blockchain Strategy a accouché de projets originaux.

L'application d'identité numérique nationale, le UAE Pass lancée en 2018 et qui ne repose pas sur l'usage d'une blockchain, propose depuis 2021 un « *Digital vault* », un coffre-fort numérique, qui permet à l'aide d'une blockchain de stocker, signer, partager et vérifier des documents avec les institutions dans tout le pays. Selon le Ministère de la Justice, la signature de documents via l'application UAE Pass aurait même une valeur notariale[50].

Autre mise en pratique intéressante, le ministère de la Santé et de la Prévention (MOHAP) a lancé en janvier 2019, avec Dhonor Healthtech, **Hayat**, un registre national des donneurs d'organe qui a vocation à remplacer le précédent système de coordination entre les autorités de chaque émirat. Avec pour objectif d'optimiser l'allocation des greffes et de limiter le trafic d'organes, Hayat aurait déjà enregistré plusieurs milliers de donneurs à l'aide de *smart contracts** dotés d'une valeur juridique aux Émirats, facilitant leur parcours, intégrant les proches comme témoins cosignataires, ainsi que celui des patients. Le registre Hayat s'appuie à la fois sur les solutions d'identité numérique officielles et sur une intelligence artificielle chargée de prioriser les attributions de greffe.

49 « Abu Dhabi Digital Authority launches Blockchain based Abu Dhabi Pay », Unlock Media, May 5, 2020, https://www.unlock-bc.com/news/2020-05-05/abu-dhabi-digital-authority-launches-blockchain-based-abu-dhabi-pay/

50 « UAE Government adopts 'blockchain' technology in authentication services », Emirates News Service, April 19, 2021, https://wam.ae/en/details/1395302928148

De plus, le MOHAP espère une économie de 20 millions de dollars par an uniquement sur la diminution des besoins de dialyses[51].

Par ailleurs, la mise en place par l'Autorité Digitale d'Abu Dhabi (ADDA) d'une plateforme blockchain nationale pour faciliter et standardiser les échanges de données au sein des entités gouvernementales et avec des partenaires externes souligne les logiques d'interopérabilité et de synergies au cœur de la stratégie. Cette solution, qui est expérimentée au sein d'une *sandbox*[52] de l'ADDA depuis 2019, instaure un niveau d'abstraction « protocole-agnostique[53] » supplémentaire permettant aux données de circuler à travers les différents systèmes blockchain utilisés dans le secteur public.

Il est relativement difficile d'estimer avec précision les effets concrets à court-terme de ces deux stratégies. Alors que le cours des années a rattrapé les horizons initialement dessinés dans chacune des stratégies, il semble qu'un écart persiste entre les très ambitieux objectifs affichés dans les discours lors des lancements et les services dont peuvent déjà bénéficier les citoyens, résidents et visiteurs des Émirats Arabes Unis. Même si quelques services publics présentés ici sont déjà en production, beaucoup d'initiatives en sont encore au stade expérimental.

L'approche « *top-down* » résolument assumée par les autorités des Émirats a probablement permis de fixer une feuille de route commune à tout le secteur public, d'allouer des ressources conséquentes et d'assurer une certaine interopérabilité entre les services qui peuvent réutiliser les solutions développées dans d'autres entités au niveau de l'émirat de Dubaï et au niveau national, mais elle a également pu causer une désynchronisation entre la stratégie gouvernementale et la réalité technologique et organisationnelle des institutions chargées d'innover à marche forcée[54].

L'enjeu de ces stratégies dépasse néanmoins l'industrialisation des expérimentations pour le pays du Golfe. D'une part, ces grands plans auront nécessairement un effet de long-terme, ne serait-ce qu'à travers les efforts d'acculturation entrepris par le gouvernement.[55]

51« Inclusive Deployment of Blockchain: Case Studies and Learnings from the United Arab Emirates », United Arab Emirates Center for the Fourth Industrial Revolution, World Economic Forum, January 2020, https://www3.weforum.org/docs/WEF_Inclusive_Deployment_of_Blockchain_Case_Studies_and_Learnings_from_the_United_Emirates.pdf

52 Sandbox : en français « bac à sable ». Dans le domaine informatique, un « bac à sable » consiste à créer un environnement de test isolé pour tester un programme.

53 Un niveau d'abstraction « protocole agnostique » désigne un environnement de développement blockchain indépendant de protocoles en particulier, permettant par la suite un portage plus simple selon les blockchains utilisées.

54 « Emirates Blockchain Strategy 2021 », GovChain, retrieved May 17, 2022, https://govchain.world/uae/

55 Le *National Programme for AI and Blockchain Capacity Building* vise, par exemple, à financer des formations pour les fonctionnaires ainsi que des programmes et des bourses universitaires.

D'autre part, l'adoption de ces stratégies relève tout autant d'une entreprise de transformation publique que d'une campagne de communication et de rayonnement pour l'État émirati afin d'asseoir sa réputation de bastion de l'innovation et des *smart cities* au Moyen-Orient, que ce soit auprès des touristes, des entreprises du numérique et des dirigeants du monde entier (*a fortiori* de ses voisins et concurrents immédiats).

Cette volonté de promouvoir les programmes d'innovation nationaux s'est faite parfois aux dépens du réalisme des objectifs affichés et au détriment de la lisibilité de l'avancement concret des projets pris individuellement. La création d'un Global Blockchain Council[56] et des investissements massifs liés à l'organisation de plusieurs conférences internationales majeures ont été annoncés pour attirer l'écosystème, capter l'attention médiatique et générer de nouvelles opportunités commerciales. A cet égard, le succès de ces opérations est déjà une réalité.

Les Émirats Arabes Unis ne sont pas les seuls à avoir lancé des projets de grande ampleur visant à expérimenter et déployer des infrastructures numériques publiques reposant sur les technologies blockchains pour moderniser son administration publique afin de faciliter l'accès à de nouveaux services publics pour les entreprises et les citoyens.

Dans le cadre de son Partenariat Européen de la Blockchain (EBP), signé le 10 avril 2018, les vingt-sept États-Membres de l'Union Européenne (à la date de la signature, Royaume-Uni compris) ainsi que la Norvège et le Liechtenstein se sont engagés à construire, ensemble, la European Blockchain Services Infrastructure, qui fait l'objet du focus de ce chapitre (voir *infra*).

Les DAOs, des laboratoires pour de nouveaux modèles de gouvernance décentralisée

Le 20 juillet 2021, Rune Christensen, l'initiateur de MakerDAO et de son crypto-actif stable* multi-collatéralisé, le Dai, dont la capitalisation a dépassé les 9 milliards d'euros en février 2022, annonce dans un billet de blog liminaire mettre un terme à la Maker Foundation. Ici, pas de scandale, pas de *fork** dramatique, pas de poursuite judiciaire.

En remettant l'intégralité de la gouvernance du protocole entre les mains de la communauté Maker organisée en DAO*, Christensen annonce « *boucler la boucle* »[57], quatre ans après le lancement de la première version de son crypto-actif stable*. Avec la suppression de la fondation, les détenteurs de MKR, le *token* de gouvernance lié au protocole, tiennent désormais en toute indépendance le gouvernail de l'un des projets-phares de la finance décentralisée (*Decentralized*

56 « Global Blockchain Council », DMCC, retrieved July 6 ,2022, https://www.dmcc.ae/about-us/global-blockchain-council
57« MakerDAO Has Come Full Circle », MakerDAO, July 20, 2021 https://blog.makerdao.com/makerdao-has-come-full-circle/

Finance, ou DeFi* - voir Chapitre « Monnaie électronique pair-à-pair et argent programmable »). En utilisant les processus de gouvernance bâtis tout au long de l'existence de MakerDAO, ils votent pour décider du destin du projet, introduisent, discutent et adoptent les *Maker Improvement Proposals*, choisissent les crypto-actifs acceptés comme collatéraux, ajustent les ratios de collatéralisation, financent de manière décentralisée les *core units*, des équipes projet avec un budget, des mandats et des objectifs, sans aucun intermédiaire, sans aucune autorité centrale.

L'exemple de MakerDAO est édifiant et inspirant pour tout l'écosystème blockchain. Il prouve que les échecs des expérimentations comme Bitnation et l'appropriation par les institutions traditionnelles publiques et privées des DLTs n'ont pas sonné le glas pour les projets portés par des communautés blockchain rejetant la centralisation, les frontières et la dépendance à des tiers.

Au contraire, il est l'une des culminations d'un mouvement de fond qui, avec l'adoption croissante d'Ethereum et d'autres protocoles démocratisant le recours aux *smart contracts**, a remis la gouvernance décentralisée sur le devant de la scène, ouvrant le champ des possibles. La grande vague des projets financés par ICO puis l'émergence de la finance décentralisée - toutes deux accompagnées par des hausses massives des cours des crypto-actifs qui ont attiré de nouveaux utilisateurs - ont notamment accouché d'une véritable explosion cambrienne des DAOs*.

Bien loin d'être découragés par l'expérience pionnière mais profondément traumatique que fut TheDAO et son piratage[58], de nouveaux projets choisissent chaque jour d'organiser l'administration de leurs ressources, de régir le fonctionnement d'un ou plusieurs services et de coordonner la prise de décision au sein de leur communauté par le biais d'une organisation décentralisée et autonome.

Plutôt que de reposer directement et exclusivement sur une structure conventionnelle avec une existence juridique (entreprise, institution publique, ONG…), les DAOs* permettent à des communautés ouvertes, transnationales, anonymes ou pseudonymes, de se rassembler autour d'un ensemble de règles et de mécanismes de gouvernance inscrits sous forme d'un ou de plusieurs *smart contracts** enregistrés dans une blockchain.

Ces communautés peuvent alors prendre des décisions stratégiques impactant la vie du projet et gérer des budgets de financement en s'affranchissant autant que possible de toute autorité centrale même si beaucoup de projets font le choix de conserver, par exemple, une fondation

58 En mai 2016, après avoir accumulé plus de l'équivalent de 150 millions de dollars, un hacker a exploité une faille dans le code pour vider ce fonds d'investissement décentralisé d'une grande partie de ses actifs, forçant même la Fondation Ethereum à un hard fork très litigieux (« The DAO (organization) », Wikipedia, retrieved July 21, 2022, https://en.wikipedia.org/wiki/The_DAO_(organization))

dûment enregistrée dans une juridiction pour des raisons juridiques, financières et opérationnelles, comme ce fut le cas de MakerDAO pendant les premières années du projet.

De l'attribution de financement à des développeurs open source à l'adoption d'une feuille de route pour un nouveau projet, de l'identification du prochain actif à ajouter sur une place de marché décentralisée* (*Decentralized Exchange* ou DEX*) à l'évolution de la courbe des taux du fonds de réserve d'un crypto-actif stable*, de l'ajout d'un artiste à une galerie d'œuvres numériques à la mise en vente d'une nouvelle parcelle vierge dans un metaverse, les DAOs* sont désormais l'un des piliers de ce que certains appellent déjà le « Web 3.0 », un internet décentralisé, fondé sur les technologies blockchains, où les utilisateurs pseudonymes retrouveraient propriété, liberté et souveraineté vis-à-vis des plateformes qui dominent le Web 2.0.

Elles regroupent parfois une poignée d'utilisateurs, parfois des milliers, pour des objectifs simples, comme par exemple la mutualisation des ressources d'une communauté pour participer à des enchères[59], ou extrêmement ambitieux, comme la gestion d'une ville ou même, dans la lignée de Bitnation, la constitution d'une *cloud nation*[60].

En juin 2022, DeepDAO recensait 4 983 DAOs* en activité, pour l'équivalent de 7,6 milliards de dollars d'actifs en gestion (la majorité de ces fonds étant concentrés dans les 183 DAOs* dont les actifs pesaient plus de un million de dollars)[61]. Huit mois plus tôt, au plus haut de la bulle des cryptoactifs, ce montant s'est même élevé à 13 milliards de dollars. Si la DeFi englobe la majeure partie de ces ressources, de nouvelles DAOs* étendent les principes de la gouvernance décentralisée dans une large diversité d'industries et de cas d'usage[62].

Les DAOs* varient dans leurs implémentations mais elles sont toutes des organisations décentralisées sans frontière ni juridiction, ce qui ne signifie pas pour autant qu'elles soient strictement « informelles ». Elles reposent, en effet, sur un ensemble de règles et de mécanismes obligatoires et contraignants compilés sous forme de code informatique dans des *smart contracts** enregistrés dans une blockchain de deuxième ou troisième génération (voir Introduction). Les décisions y sont le plus souvent prises *via* des votes de la communauté dont l'exécution des résultats est, grâce aux *smart contracts*,* automatique et transparente.

59 Plusieurs DAOs ont vu le jour comme un véhicule de financement participatif, comme pour acheter l'une des copies originales de la constitution américaine, sans succès, contrairement à l'achat du script du film Dune imaginé par Jodorowsky, ou encore pour lever 6,7 millions de dollars à destination de l'ONG ukrainienne Come Back Alive.
60 « Building a DAO governed Crypto City », City DAO, retrieved July 21, 2022, https://www.citydao.io/ ; « A New Nation State on the Cloud », Nation3, retrieved July 21, 2022, https://nation3.org/
61 « Organizations », DeepDAO, retrieved May 17, 2022, https://deepdao.io/organizations
62 « 15 ways the world is transformed by DAOs », Aragon, July 6, 2021, https://blog.aragon.org/15-ways-the-world-is-being-transformed-by-daos/#metaverses-virtual-worlds

Elles sont souvent articulées à des instances de discussion et des processus de coordination dits « *off-chain* », en dehors de la blockchain. A la manière des BIPs, les propositions sont souvent d'abord introduites et discutées dans des forums ou sur des réseaux sociaux plus ou moins ouverts (Twitter, Discord, Telegram…) avant d'être soumises au vote pour s'assurer de leur pertinence et faciliter la coopération au sein de la communauté.

Ce fonctionnement ouvert et collaboratif est souvent revendiqué comme démocratique et horizontal. S'il est évident que les DAOs* représentent aujourd'hui de fascinants laboratoires de modèles de gouvernance alternatifs, les variations dans les modes de scrutins établissent des distinctions fondamentales et dessinent un paysage beaucoup plus nuancé.

Puisque les DAOs* ne peuvent pas établir de « listes électorales » centralisées comme le feraient des états ayant accès à l'identité physique des votants, c'est la détention d'un crypto-actif ou le placement de ce crypto-actif dans un fonds en l'échange d'un *token* de gouvernance qui permet de prouver son appartenance à une communauté ouverte, et donc son droit à participer aux votes de la DAOs* sans nécessité de révéler son identité. Dans la plupart des cas, le poids de chaque vote dans les résultats est même pondéré en fonction de la quantité de *tokens* détenus par chaque utilisateur. Ces votes basés sur l'enjeu (*stake-based)*, permettent de garantir l'ouverture et la décentralisation du système, puisqu'un utilisateur peut acquérir des *tokens* et intégrer le processus de décision à tout moment, mais aussi de limiter certaines attaques (usurpation d'identité, bourrage d'urnes…) et de s'assurer que chaque personne participant au vote a un réel intérêt à voir le projet se développer et la valeur de ses actifs s'apprécier. *A contrario*, le coût d'une tentative de subversion du système par un acteur malveillant est d'autant plus élevé qu'il lui est nécessaire d'acquérir des *tokens* et de les utiliser d'une manière qui pourrait leur faire perdre de la valeur.

Dans les faits, ce type de gouvernance, souvent présentée comme « méritocratique », présente des biais structurels et peut rapidement dégénérer en ploutocratie. Le niveau de participation dans les DAOs* est souvent limité. Les votes sont nombreux, parfois plusieurs par semaine, et les utilisateurs ne possédant qu'un petit *stake** n'ont qu'un faible intérêt à investir le temps et l'attention nécessaires à une participation régulière.

Par opposition, les « *whales* »[63] bénéficient d'un poids colossal dans la gouvernance d'une DAO*, surtout si, en tant que *early investors*, elles ont acquis les *tokens* à des prix très avantageux avant leur distribution ou leur mise sur le marché[64].

63 « Baleines » en français, surnom donné aux gros portefeuilles possédant une grande quantité de crypto-actifs

64 Dans le cas de Compound, les quatre adresses détentrices du plus gros stake sont des fonds d'investissement, les 5 et 6èmes appartenant aux co-fondateurs de Compound Labs, l'entreprise derrière Compound. Ils représentent à eux six, au moment de l'écriture, plus de 40% de la quantité totale des votes

Pour faire face à la « fatigue électorale » ou au « désintérêt rationnel » des petites parties prenantes, pour assurer un éventuel quorum et pour augmenter la légitimité des décisions d'une DAO*, nombreuses sont celles qui autorisent la délégation des votes[65]. Ce processus permet d'augmenter la participation de la communauté, mais tend encore à renforcer le pouvoir des *whales* qui, parce qu'elles ont les ressources pour s'investir continuellement dans la gouvernance d'une ou plusieurs DAOs* et parce qu'elles sont souvent très visibles dans les forums et sur le « CryptoTwitter », sont des récipiendaires logiques pour les délégations.

Ce genre de barrières à l'entrée peut même intervenir plus en amont dans le processus de gouvernance. **Compound**, l'une des principales solutions de marché monétaire (*money market*) décentralisé dont le modèle de gouvernance a été repris par de nombreuses DAOs* (Uniswap, Radicle…) requiert que toute proposition de modification du *smart contract* soit soumise par une adresse possédant ou à laquelle ont été délégués au moins 25 000 COMP (la valeur du COMP oscille entre 150 et 30 dollars au 2e trimestre 2022, après avoir dépassé les 800 dollars en mai 2011)[66]. Cette mesure, initialement mise en place pour limiter les risques de *spam* et s'assurer que les propositions auraient un soutien minimal avant d'être mise au vote, force d'éventuels petits acteurs à convaincre la communauté pour recevoir les délégations avant même de pouvoir soumettre une proposition au vote, ou bien de s'appuyer sur l'une des *whales* pour introduire la proposition en leur nom.

Il faut cependant noter que Compound a mis en place d'autres moyens de participer à la gouvernance, notamment la possibilité d'amorcer une proposition avec seulement 100 COMP via un *smart contract** recueillant ensuite les délégations nécessaires pour valider le plancher évoqué plus haut, ainsi que la mise en place d'une liste blanche par laquelle la communauté autorise un nombre restreint de contributeurs réguliers à proposer des évolutions sans avoir à valider les seuils de délégation évoqués plus haut.

La gouvernance décentralisée peut souffrir d'autres biais tout aussi problématiques. Les votes étant publiquement accessibles sur une blockchain, même avant la clôture d'une votation, la prise de position d'un de ces gros portefeuilles peut influencer les résultats finaux et donner une image biaisée du consensus, par exemple en décourageant totalement la participation de petits utilisateurs qui pourraient être pourtant opposés à la mesure soumise au vote. Les processus de délégation peuvent même renforcer ce biais, l'engagement du délégataire ne reflétant pas forcément

disponibles.

65 Système de vote dans lequel les utilisateurs d'une blockchain votent pour des représentants chargés de valider les blocs à leur place.

66 Ce plancher s'élevait originellement à 100k COMP, avant d'être descendu à 65k en juillet 2021 puis 25k en mars 2022, le nombre d'adresses capables de sponsoriser une proposition passant de moins d'une dizaine, à une dizaine puis à une trentaine d'adresses.

l'opinion ou l'absence d'opinion des individus qu'il représente.

Un autre point critique est celui de la publicité des scrutins, qui peut faciliter l'achat de voix et la mise en place de systèmes de corruption organisés. Puisque la participation d'une adresse publique à un vote ainsi que son choix peuvent être vérifiés, n'importe qui peut proposer de récompenser certains comportements afin d'influencer sur la gouvernance d'une DAO*[67].

Mieux encore : avec l'explosion de la valeur de la DeFi et les enjeux financiers grandissants impliqués dans les protocoles de gouvernance décentralisé, plusieurs plateformes comme Convex[68] ou le bien nommé Bribe ont même fait leur apparition, proposant tout simplement aux propriétaires de *token* de gouvernance des systèmes d'achat de votes décentralisés et automatisés[69].

Des attaques encore moins « subtiles » sont rendues possibles par certains systèmes de votes fondés sur la détention de crypto-actifs : si les *tokens* sont largement accessibles et liquides, un utilisateur extérieur à la communauté peut très bien acheter puis revendre ou emprunter une grande quantité de tokens afin de proposer et/ou de voter une mesure favorable à son intérêt personnel, au détriment du bien à court ou long terme de la DAO* concernée[70].

Plusieurs alternatives ont néanmoins été proposées afin de rendre la participation aux DAOs* structurellement plus démocratique. Certaines DAOs* ont adopté le vote quadratique, un système où chaque électeur dispose d'un « crédit » de plusieurs voix à distribuer dans un ou plusieurs votes. Un électeur peut allouer l'intégralité de ses voix à un seul choix, mais le coût de chaque vote additionnel augmente de manière quadratique (ou inversement, le poids de chaque nouvelle voix diminue de manière quadratique).

Ce type de scrutin, tout en autorisant l'asymétrie du « *stake** » à la disposition de chaque votant, favorise donc les choix recueillant l'assentiment du plus grand nombre de participants.[71]

En proposant une plateforme d'investissement participatif où les contributions sont abondées par un fond selon un système de « *matching* »

67 Dans un article de juillet 2018, *On-Chain Vote Buying and the Rise of Dark DAOs*, Daian, Kell, Miers et Juels listaient déjà plusieurs raisons structurelles pour lesquelles les systèmes de votes sur des blockchain publiques peuvent permettre la mise en place de marché d'achat de votes efficaces et automatisés, directement dans une blockchain avec des *smart contracts* dédiés, ou bien *off-chain*.
68 « How it works », Convex, July 6, 2022, https://www.convexfinance.com
69 « Pay-to-Play Governance Builds Steam as Bribe Raises $4M », Andrew Thurman, Coindesk, January 22, 2022, https://www.coindesk.com/tech/2022/01/12/pay-to-play-governance-builds-steam-as-bribe-raises-4m/
70 Justin Sun, le sulfureux fondateur de la blockchain Tron, s'est fait une spécialité de ces tentatives de subversion de la gouvernance décentralisée en exploitant les plateformes d'échange pour acquérir un *stake** important et forcer des décisions favorisant Tron et les services qui y sont construits, d'abord avec la rocambolesque affaire Steem, puis plus récemment avec MakerDAO et Compound.
71Il faut noter que ce mode de scrutin peut faire l'objet « d'attaques Sybil ».

quadratique[72], **Gitcoin** a permis l'allocation de l'équivalent de plus de 50 millions de dollars à destination de projets open source de « bien public » dans l'écosystème blockchain[73].

D'autres initiatives tentent de réconcilier le vote dans les DAOs* et les processus démocratiques en substituant la pondération des votes en fonction des actifs détenus par de nouveaux outils d'authentification. Ces alternatives au « *coin voting* » entendent empêcher les « attaques Sybil »[74] et rétablir l'égalité « un vote pour un utilisateur » en prouvant qu'une clé publique est bien liée à un unique membre de la communauté, sans pour autant dévoiler son identité.

Outre les projets de *self-sovereign identity* (SSI, voire chapitre « Identité et propriété), POAP, pour *Proof of Attendance Protocol*, permet par exemple d'attribuer aux membres un NFT selon leur activité réelle dans leur communauté, tels que des contributions au code source d'un projet, à son wiki ou à son forum, par l'organisation d'événements ou par la participation à ceux-ci. Ce type de NFT*, qui reste toutefois difficile à attribuer de manière strictement décentralisée sans système d'identification liant l'identité *off-chain* et *on-chain* (par exemple, entre un compte Github et une adresse publique sur la chaîne utilisée), peut alors servir de droit de vote dans la DAO* sans nécessiter d'investissement financier, en complément ou en remplacement du vote par participation « *stake** ».

Dans une veine similaire, **Snapshot** (voir *infra*) et **Orange Protocol** ont annoncé un partenariat ayant pour objectif de proposer aux DAOs* de pondérer les votes de leur communauté en fonction de la réputation de chaque propriétaire de *tokens*.

La fondation **democracy.earth** veut aller encore plus loin avec son projet « Proof of Humanity », un système d'identité décentralisée où n'importe quel être humain peut obtenir une identité numérique unique qu'il peut ensuite faire valoir dans des communautés sur une blockchain (Voir chapitre « Identité et propriété ». Pour intégrer la liste « Sybil-résistante » de véritables êtres humains, portée par le projet, tout utilisateur doit au moins fournir un nom par lequel il est connu (ce nom n'étant pas forcément celui déclaré à l'État-civil), ainsi qu'une photo de son visage et une vidéo dans laquelle il ou elle tient un support présentant l'adresse Ethereum qui portera la « preuve d'humanité » et déclare, à visage découvert et d'une voix audible : « *I certify that I am a real human and that I am not already registered in this registry*[75] ». Une fois une caution payée, la vérification de chaque demande est assurée par la communauté, en pair-à-pair.

72 Dans un tel système, si un projet reçoit une contribution de $100 et un autre 10 contributions de $10, alors le premier projet recevra un abondement de $10 de la part du fonds Gitcoin, le second de $190.
73 « Gitcoin is the community of builders, creators, and protocols at the center of open web ecosystems », Gitcoin, retrieved May 17, 2022, https://gitcoin.co/about
74 La création de multiples identités numériques liées à ou contrôlées par une seule entité.
75 « Je certifie être un véritable être humain et ne pas être déjà enregistré dans le répertoire ».

Tout membre déjà authentifié peut valider la demande ou la remettre en question s'il l'estime invalide ou fausse (doublon, personne inexistante ou décédée…). En cas de validation, la caution est remboursée, et l'utilisateur bénéficie d'une clé publique attestée comme appartenant à un être humain unique, ainsi que le droit de recevoir des tokens UBI (Universal Basic Income), un système de « revenu universel » porté par democracy.earth. En cas de contestation, la dispute est soumise à une cour d'arbitrage également décentralisée, *via* le protocole Kleros. En cas de rejet de la demande, c'est le membre de la communauté à l'origine de la contestation qui récupère alors la caution pour le récompenser de sa vigilance.

Il est intriguant de noter que, si les défenseurs de la DeFi et du Web 3.0 considèrent les inégalités ou barrières financières, que ce soit dans les équilibres de vote mais aussi parfois pour pouvoir soumettre une proposition à la DAO*, elles sont relativement naturelles voire bénéfiques en matière de gouvernance décentralisée, puisqu'elles permettent d'aligner l'engagement des parties prenantes à la hauteur de leur « intéressement » dans le succès d'un projet, beaucoup d'efforts ont été investis pour diminuer drastiquement les barrières techniques qui pourraient effrayer les investisseurs comme les porteurs de projets.

De nombreux services comme **Tally** ou **Boardroom** proposent aux investisseurs des interfaces faciles d'utilisation pour suivre les propositions et les votes, en cours et passés, qui ont lieu dans les principales DAO*. Avec l'augmentation des frais de transaction et donc du coût des votes *on-chain*, des solutions de consultations alternatives émergent, comme notamment **Snapshot**, qui permet à plus de 6 000 organisations d'héberger des propositions et de les voter (ou plutôt de « signaler ») *off-chain* mais de manière décentralisée, à l'aide du protocole InterPlanetary File System (IPFS*) (voir également le Chapitre Web 3.0, arts et sciences). Snapshot consulte les données sur une blockchain pour établir les « listes électorales » et pondérer le poids de chaque vote conformément au nombre de *tokens* détenus.

Il permet surtout aux DAOs* de tester l'opinion de leurs communautés avant de lancer un vote contraignant et coûteux sur leur infrastructure blockchain. La multiplication de services ayant pour but de faciliter la création de nouvelles DAOs* est encore plus symptomatique de cette vague de démocratisation de la gouvernance décentralisée.

Ces plateformes, elles-mêmes régies par des DAOs*, mettent à disposition de tous des outils open source qui ne nécessitent pas forcément de connaissance technique (*no-code*) et s'érigent aujourd'hui comme des standards dans l'écosystème blockchain. Ces outils permettent de générer des *smart contracts** suivant le modèle de gouvernance choisi et de les paramétrer pour administrer la vie de chaque projet.

Un petit tour d'horizon non-exhaustif de ces plateformes de lancement de DAOs* permet d'en saisir les particularités.

DAOhaus offre la possibilité à quiconque de créer sa propre DAO* sur Ethereum, Gnosis, Polygon, Arbitrum ou encore Celo, selon le standard Moloch, apparu en 2019 notamment pour administrer des fonds de manière décentralisée[76]. DAOhaus propose à ses utilisateurs cinq modèles, aisément adaptables ensuite avec une demi-douzaine de paramètres. Cette simplicité d'usage a permis le lancement d'environ 2 000 DAOs* à la fin 2021, pour plus de 10 000 adresses uniques membres de ces organisations[77]. Les DAOs* peuvent accéder à de nouvelles fonctionnalités *via* des plugins additionnels appelés « Boosts » qui pourront faire appel à des *smart contracts** externes *via* les « Minions[78] ».

DAOstack est une autre plateforme *open source* de génération de DAOs*. Son outil Alchemy permet également de créer des DAOs* en quelques clics et se distingue surtout par la possibilité d'implémenter des outils de « consensus holographique »[79] avec le *token* GEN, natif de cette plateforme. La hiérarchisation des priorités est ainsi facilitée au sein d'une organisation, les utilisateurs de DAO* créées sur DAOstack peuvent parier leurs GEN sur les propositions dont l'adoption leur semble la plus probable. Ce « marché de la prédiction » appliqué à la gouvernance, directement inspiré par le concept de « futarchie »[80], aurait donc pour vertu d'agréger les intérêts divergents au sein de la communauté et de donner rapidement une plus grande visibilité aux propositions les plus consensuelles, ou tout du moins les plus susceptibles d'être soutenues par la majorité. Malgré cette fonctionnalité, DAOstack ne s'est jamais vraiment imposé et ne semble plus jouir d'une activité foisonnante.

Le bouillonnement autour des DAOs* est tel que certaines plateformes s'adressent principalement à un seul type de cas d'usage. Juicebox se concentre ainsi sur les DAOs* ayant pour but de servir d'outil de financement participatif. Son interface graphique attrayante donne accès à un ensemble de paramètres pour ajuster les variables économiques liées au projet et ses *tokenomics*[81].

76 Moloch inclut notamment un mécanisme de protection des investisseurs minoritaires dans la DAO : le ragequit donne aux utilisateurs la possibilité de « claquer la porte » d'une DAO en cas de désaccord irréconciliable avec une décision adoptée mais pas encore implémentée, en emportant avec eux une part des fonds proportionnelle à leur poids dans la gouvernance.
77« 2021 Year in Review », DAOHaus, retrieved May 17, 2022, https://daohaus.club/review/
78 « *Les minions permettent à votre DAO d'appeler des contrats arbitraires, ce qui vous permet de faire de nombreuses choses comme gérer les Ethereum Name Service, collecter les NFT, gérer la trésorerie dans la DeFi, etc.* ». « Minion FAQ », Minion, retrieved July 21, 2022, https://daohaus.club/docs/users/minion-faq/
79« Holographic Consensus - part 1 », Matan Field, Medium, November 12, 2018, https://medium.com/daostack/holographic-consensus-part-1-116a73ba1e1c
80« Futarchy: Vote Values, But Bet Beliefs », Robin Hanson, mason.gmu.edu, retrieved May 17, 2022, http://mason.gmu.edu/~rhanson/futarchy.html
81*Tokenomics* : contraction de *Token* et *Economics.* Définit les règles de fonctionnement d'un token et de ses

Juicebox fait également office de répertoire pour les plus de 600 projets qui ont été créés sur cette plateforme et qui financent, en retour, grâce à des frais sur chaque retrait du trésor d'une DAO* (2,5 %), celui de la JuiceboxDAO.

De toutes ces plateformes « meta-DAOs », **Aragon** est, avec DAOhaus, la plus influente. Durant l'année 2021, plus de 1 000 DAOs* ont été créées avec Aragon (principalement sur Polygon, Ethereum ou Harmony). Fondé en 2016 avec comme mission de garantir la liberté et la souveraineté des individus et des communautés en ligne en fournissant gratuitement de nouveaux outils de coordination et de gouvernance décentralisée, Aragon se distingue par sa « suite » d'outils intégrés verticalement, pour couvrir tous les besoins de gouvernance d'une organisation fonctionnant de manière décentralisée.

Aragon Client permet de paramétrer et déployer facilement sa DAO*. Aragon Connect permet d'interfacer cette DAO* à d'autres applications. Aragon Court prend le relais en cas de blocage et propose un système d'arbitrage décentralisé pour résoudre les disputes qui auraient lieu au sein des DAOs*. Cet outil organise un réseau de « *guardians* » qui suivent un processus défini de nomination, de réception et d'évaluation des litiges, pour lesquels un jury est sélectionné, débat puis vote pour émettre un arbitrage, avec la possibilité de faire appel. Plus récemment, Aragon a lancé Voice, son outil de vote *off-chain* venant concurrencer Snapshot, ainsi que Govern, un nouvel outil de création et de gestion de DAO* qui a pour but de surpasser les standards utilisés par Client avec un système de gouvernance « optimiste », beaucoup plus économique en termes de frais (*gas*) sur une blockchain[82].

Enfin, Aragon a également racheté, en juillet 2021, **Vocdoni**, une *startup* catalane développant des outils de gouvernance décentralisée et de vote électronique à destination d'associations et d'organisations politiques traditionnelles. L'intégration de Vocdoni par Aragon souligne le foisonnement actuel en matière de DAOs* et la perméabilité qui existe entre les efforts de développement de la gouvernance décentralisée pour l'écosystème « Web3.0 » et ceux des institutions publiques et de la société civile.

variables économiques et de gouvernance.

82 Avec Govern, les DAOs peuvent choisir des acteurs comme executors, leur donnant la permission d'initier des actions (par exemple après un vote préalable off-chain sur Voice) sans passer par un vote on-chain. Ces décisions sont implémentées après un délai durant lequel les membres de la communauté peuvent contester la mesure à l'aide de Aragon Court. Cette division des pouvoirs entre des branches délibératives, exécutives et juridiques qui répondent à des contraintes économiques et techniques (explosion des coûts du gas) ainsi qu'organisationnelle (votes à répétition, mêmes pour des mesures consensuelles) en réintroduisant des structures de gouvernance hiérarchisées qui nous sont familières est absolument fascinante.

Focus *European Blockchain Service Infrastructure* (EBSI)

Peu de projets font aussi bien la synthèse entre les dynamiques liant blockchain et démocratie, décrites dans ce chapitre que le European Blockchain Service Infrastructure (EBSI). Cette mesure-phare du Partenariat Européen de la Blockchain (*European Blockchain Partnership* - EBP) signé le 10 avril 2018 par tous les États membres de l'UE, rejoints par la Norvège et le Liechtenstein, a pour objectif de s'inscrire dans l'élan général du plan de financement Connecting Europe Facility (CEF) et de créer une infrastructure européenne fondée sur les technologies blockchains afin d'accueillir une nouvelle génération de services publics numériques paneuropéens.

L'EBSI permet de rassembler tous les États membres dans une dynamique partagée d'identification de cas d'usage communs et de proposition de solutions au service de tous les citoyens européens. Ces solutions ne se contentent pas d'être de simples « portages » de services publics sur une blockchain, dans une éventuelle dynamique de modernisation de l'existant. L'EBSI est engagée dans une démarche d'innovation, voire d'invention de services transfrontaliers reposant, certes, toujours sur des tiers de confiance mais pour lesquels la transparence, la décentralisation, la sécurité et l'interopérabilité apportée par une blockchain est à même de renforcer la valeur ajoutée pour les citoyens.

Cette infrastructure est articulée autour de cinq principes clés : la poursuite du bien public, la mise en place d'une gouvernance partagée, la proposition et l'adoption de standards harmonisés, le développement open source ainsi que le respect du droit européen, tout particulièrement en matière de protection des données.

Le choix de l'*open source* et la volonté de créer des standards interopérables à l'échelle européenne plutôt que de laisser les administrations de chaque État membre tenter de construire de nouvelles infrastructures de manière fragmentaire, sont des facteurs essentiels pour le succès de l'EBSI. Non seulement cette démarche collaborative mutualise en partie les coûts de R&D et d'infrastructure, mais elle permet également de démultiplier l'impact potentiel des projets en facilitant le passage à l'échelle des expérimentations.

Elle rend également possible la coopération avec l'écosystème d'innovation européen, directement associé aux démarches de conception et à la création des standards, que les *startups* ont un intérêt direct à adopter pour construire de nouvelles offres capables de s'adresser au grand public européen sur cette infrastructure qui se revendique adaptée au marché (*market-friendly*).

L'EBSI, qui bénéficie au total de 38 millions d'euros d'investissements pour l'année 2021-2022[83], prend aujourd'hui la forme d'un réseau blockchain permissionné de 36 nœuds opérés par les institutions publiques de 23 pays signataires du Partenariat Européen de la Blockchain (*European Blockchain Partnership* - EBP), fonctionnant avec les protocoles de consensus Hyperledger Besu et Fabric (PoA). Côté écosystème, une dizaine de portefeuilles* (*wallets*) sont déjà compatibles avec l'EBSI.

L'architecture technique de l'EBSI comprend, par-dessus cette infrastructure qui assure la connexion à cette blockchain européenne et, à termes, avec d'autres réseaux blockchain interopérables, y compris publics, une couche « *chain* et stockage *off-chain* » où sont enregistrées les données chiffrées impliquées dans les cas d'usage, et une couche « *core services* » qui rassemble des API standardisés conçues pour faciliter le développement d'applications de service.
Les cas d'usage appréhendés dans le cadre de l'EBSI ont comme leitmotiv de passer d'un modèle de partage de données et de vérification tout deux centralisés à un système similaire à la *self-sovereign identity*.

Plutôt que de recevoir d'un tiers de confiance un document qui doit toujours être vérifié auprès de l'émetteur, les utilisateurs d'un service de l'EBSI sollicitent des tiers de confiance pour générer des certificats numériques vérifiables (*verifiable credentials*) qu'il conserve dans leur *wallet** et dont l'authenticité peut être confirmée par le destinataire directement via l'EBSI grâce à des techniques de chiffrement.

Ces certificats, respectent le standard global W3C et seront normalement reconnus à travers l'Europe. Ils ont le potentiel de rendre aux utilisateurs la propriété et le contrôle de leurs données personnelles qu'ils pourraient partager de manière sélective et « atomique », en ne révélant qu'un seul attribut d'identité (par exemple, le fait que l'utilisateur a plus de 18 ans), sans révéler les autres informations contenues dans le document qu'ils auraient transmis à leur interlocuteur (selon le même exemple, sans dévoiler les autres informations contenues dans une pièce d'identité, pas même la date de naissance). L'EBSI doit également permettre de diminuer les risques de fraude et les délais de vérification, surtout dans le cadre de procédures transfrontalières.

Sept cas d'usage ont été prioritairement identifiés par les membres du Partenariat Européen de la Blockchain. Une première vague d'expérimentations est consacrée aux cas de la notarisation numérique, de l'identité auto-souveraine (voir Chapitre « Identité et propriété »), de la gestion des diplômes et des certificats de formation, ainsi qu'à la mise en place d'un identifiant

83 « Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021 – 2022 », European Commision, November 10, 2021, https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf

de sécurité sociale européen unique (European Social Security Pass, ESSP). Dans un deuxième temps, les efforts seront bientôt étendus au traitement des demandes de droit d'asile, à une plateforme européenne de financement obligataire des PME et aux solutions de partage sécurisé des données (Trust Data Sharing).

En fédérant les États européens autour d'une infrastructure commune et des standards *open source*, en associant l'écosystème d'innovation à la conception de nouveaux services publics interopérables, l'EBSI constitue un exemple remarquable d'utilisation des technologies blockchains pour moderniser l'action publique et pour renforcer la confiance, non seulement entre les institutions et les citoyens, mais aussi potentiellement entre tous les acteurs du Marché Unique Numérique européen. La démarche de l'EBSI transcende les limites de la plupart des projets qui l'ont précédée en matière de blockchain et de e-gouvernement.

La vision qu'elle porte est profondément enracinée dans les valeurs européennes de transparence, de confiance, de liberté et de respect de la vie privée. Elle s'articule aussi avec les réglementations numériques de l'Union, tout en mobilisant des ressources au niveau national et continental. En plus de sa cohérence, l'EBSI bénéficie également de sa taille. Alors que les technologies blockchains peinent encore à se démocratiser et à pénétrer les habitudes du grand public (surtout hors des usages financiers), la base d'utilisateurs potentielle de l'EBSI est forcément un atout : elle permet aux institutions et aux entreprises innovantes européennes de construire des services qui ont le potentiel d'atteindre rapidement une large population d'utilisateurs, tout en réduisant le coût d'entrée pour les administrations à la traîne ou dotées de budgets insuffisants pour investir dans des efforts de R&D de leur côté.

Surtout, alors que l'appareil législatif européen s'efforce de mieux réguler les géants du numérique, le déploiement de l'EBSI relève des enjeux de la souveraineté et de l'intégration européennes. Car en utilisant les technologies blockchains pour construire des services accessibles à tous les citoyens et toutes les entreprises à travers l'Europe, des services décentralisés, où les institutions publiques génèrent durablement de la confiance et organisent une gouvernance démocratique, transparente et partagée, fondée sur des valeurs européennes fortes, des services où l'utilisateur est placé au centre, est propriétaire de ses propres données et libre dans ses usages, l'EBSI propose un système qui peut renforcer la souveraineté et l'indépendance technologique de ses États tout en protégeant celles de ses citoyens.

Il est trop tôt pour dire si l'EBSI va atteindre ses objectifs, si nous utiliserons au quotidien, dans les années à venir les services qu'elle développe. Comme tous les projets d'innovation, l'EBSI implique de l'incertitude, le risque de parier sur les mauvais standards, de manquer des investissements correspondants à ses ambitions.

Le projet devra survivre aux aléas liés à sa gouvernance collaborative associant une trentaine d'États avec des politiques nationales et des contextes économiques différents, sans tomber dans une lenteur handicapante pour un écosystème aussi bouillonnant que celui des technologies blockchains.

Mais si l'EBSI réussit à fournir des services efficaces et accessibles à tous, alors ce modèle pourrait non seulement transformer les modes de vie numérique des citoyens européens, mais sa vision et ses standards pourraient également s'exporter au-delà des frontières de l'Europe[84], contribuer à l'émergence de services publics interopérables partout dans le monde et constituer l'un des piliers sur lesquels ériger un autre Internet, plus décentralisé, plus ouvert, où les utilisateurs peuvent interagir en ligne avec des partenaires publics comme privés, tout en restant maîtres de leurs données et libres de leurs choix d'outils et de services.

84 A la manière, par exemple, du RGPD, comme décrit par Anu Bradford dans son fameux livre The Brussels effect, https://www.brusselseffect.com/.

ENJEUX ET QUESTIONS

De l'émergence des crypto-actifs et des technologies de registre distribué comme alternatives aux tiers de confiance traditionnels jusqu'au foisonnement actuel de DAOs* et de leurs modèles de gouvernance décentralisée, des premières expérimentations étatiques essaient de mettre les technologies blockchains au service de leur digitalisation jusqu'à la mise en place d'infrastructures *open source* de grande ampleur où les institutions publiques et *startups* collaborent.

Les liens entre blockchain, e-gouvernement et démocratie dessinent une dialectique remarquable entre un écosystème d'innovation rassemblant des individus, parfois pseudonymes ou anonymes, sous la bannière transnationale (voire a-nationale) d'une entreprise, d'une DAO* ou d'un groupe informel et des États qui, avec leurs administrations historiques, sont en quête de modernisation face à la place grandissante que prennent les technologies numériques dans l'organisation de nos sociétés.

Pour comprendre en quoi cette forme de concurrence pour des systèmes de gouvernance plus horizontaux et des services publics plus transparents, plus efficaces est absolument essentielle, elle doit être replacée dans le contexte actuel.

D'une part, les GAFAM[1] et autres « Big Tech » ont accumulé des pouvoirs immenses et régissent au moins en partie nos activités numériques en s'affirmant comme les médiateurs d'une part croissante de nos rapports socio-économiques au monde.

En même temps, nos démocraties traversent une crise fondamentale, avec une érosion profonde de la confiance envers les tiers de confiance et figures d'autorité, qu'elles soient scientifiques, médiatiques et bien évidemment politiques.

D'après la méta-analyse du *Centre for the Future of Democracy*, le taux moyen d'insatisfaction envers la démocratie, mesuré dans 77 pays démocratiques, s'établit à 57,5 %[2].

1 GAFAM, acronyme des géants de la tech, Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft.
2 « Global Satisfaction with democracy », Foa, R.S., Klassen, A., Slade, M., Rand, A. and R. Collins, Bennett Institute for Public Policy of the University of Cambridge, January 2020, https://www.cam.ac.uk/system/files/report2020_003.pdf

Selon le Pew Research Center, plus des deux tiers de la population des États-Unis, de l'Italie, de l'Espagne, de la Grèce, de la France, de la Belgique, de la Corée du Sud et du Japon estiment que leur système politique doit être complètement réformé ou a besoin de transformations majeures[3].

Il existe donc aujourd'hui un besoin réel pour de nouvelles formes de gouvernance plus participatives, transparentes et décentralisées. Cette aspiration était déjà au cœur du terreau idéologique originel des technologies blockchains et elle se concrétise au moins partiellement dans l'effervescente émergence des DAOs* et de la myriade de systèmes de gouvernance décentralisée qu'elles adoptent. Il serait néanmoins injuste de juger du potentiel de ces nouvelles formes de gouvernance décentralisée uniquement à la lumière du très imparfait état actuel des DAOs*. Déjà parce que toutes n'ont pas pour ambition d'être démocratiques.

L'influence de la pensée libertarienne et de l'anarcho-capitalisme sur l'écosystème blockchain, la création soudaine d'une quantité astronomique de valeur et la dépendance aux systèmes de vote par immobilisation (*staking**) poussent certaines DAOs* à accepter des inégalités et une centralisation ploutocratique, qui peuvent être incompatibles avec le bon exercice de la démocratie[4].

Ensuite parce que de nombreuses voix s'élèvent aujourd'hui pour souligner ces problèmes[5], y compris certains qui sont communs à nos démocraties constituées (financement des biens publics, lutte contre la corruption, centralisation du pouvoir politique dans les mains des plus fortunés…) et de proposer des solutions innovantes.

Enfin, ce n'est pas une injure pour la gouvernance décentralisée que de souligner son immaturité : les sociétés démocratiques sont le résultat de siècles d'expérimentations et de conflits, il est naturel que la recomposition promise par les DAOs*

3 « Citizens in Advanced Economies Want Significant Changes to Their Political Systems », Richard Wike, Janell Fetterolf, Shannon Schumacher and J.J. Moncus, pewresearch.org, October 21, 2021, https://www.pewresearch.org/global/2021/10/21/citizens-in-advanced-economies-want-significant-changes-to-their-political-systems/

4« Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream », Primavera De Filippi, Decentralized Thriving : Governance and Community on the Web 3.0, February 19, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524352

5« Moving beyond coin voting governance », Vitalik Buterin, Vitalik's Buterin website, August 16, 2021, https://vitalik.ca/general/2021/08/16/voting3.html

ne résolvent pas instantanément tous les problèmes sur lesquels nos États butent et trébuchent.

Plutôt que d'embrasser la caricature d'un « vieux monde » soudainement bouleversé par des organisations cyberpunks, ou bien celle tout aussi peu pertinente consistant à nier l'intérêt et la nouveauté des DAOs*, il faut souligner la porosité qui existe entre ces deux univers. La gouvernance décentralisée, qui partage beaucoup de contraintes avec nos institutions publiques, représente une magnifique opportunité de remise en question, de déconstruction et de reconfiguration de nos systèmes démocratiques en crise.

Les DAOs* sont de fantastiques laboratoires pour tester des technologies qui peuvent apporter plus de résilience, de transparence et d'efficacité à nos administrations et aux services publics qu'ils doivent délivrer.

Elles permettent surtout d'expérimenter des modèles de vote et de gouvernance alternatifs, polycentriques et souverains, pour les États et surtout pour les citoyens, qui peuvent ensuite être adoptés, même éventuellement sans infrastructure blockchain, par nos institutions (les DAOs* stimulent la recherche sur des concepts comme la démocratie liquide et le vote quadratique qui, par exemple, a été utilisé en 2019 par les sénateurs démocrates du Colorado pour préparer leur lois budgétaires[6]).

Enfin, tout comme la concurrence que représente l'usage de la gouvernance décentralisée peut être le déclencheur vertueux d'un sursaut démocratique pour nos États, les DAOs* ont paradoxalement, elles aussi, beaucoup à gagner d'un tel rapprochement.

Les mécanismes de gouvernance de celles-ci reposent sur la « tokenisation » des droits des utilisateurs et de leur poids dans les organisations. Avec les logiques de maximisation du profit inhérentes aux technologies blockchains et aux principes de théorie des jeux qui sont au cœur de leurs protocoles de consensus, les DAOs* peuvent parfois dériver vers une « sur-financiarisation » de leur gouvernance.

Les logiques financières, voire spéculatives, peuvent prendre le pas sur les objectifs de décentralisation, d'horizontalité, d'indépendance

6 « Colorado Tried a New Way to Vote: Make People Pay—Quadratically », Adam Rogers, Wired, April,16 2019, https://www.wired.com/story/colorado-quadratic-voting-experiment/

ou de transparence dans ces communautés, justifiant même des systèmes très défaillants qui paraîtraient injustes ou scandaleux dans des sociétés démocratiques.

Par exemple, les marchés d'achat et de vente de droits de gouvernance comme Bribe[7] rendent peut-être plus visibles des phénomènes de corruption qui existent bel et bien hors des écosystèmes blockchains, ils n'en restent pas moins clairement des dérives, des symptômes de risques à prendre en compte dans la conception, le développement et l'adoption de nouveaux systèmes de gouvernance décentralisée crédibles, résilients et désirables.

Les États ont ainsi des enseignements à tirer des DAOs* mais les DAOs* ont également beaucoup à gagner en s'inspirant des processus démocratiques existants. A cet égard, une initiative comme celle de l'*European Blockchain Service Infrastructure* (EBSI) laisse entrevoir le potentiel que peut avoir le déploiement de services publics reposant sur des technologies blockchains.

Elle peut être à l'origine d'un élan de standardisation et de démocratisation de ces technologies auprès du grand public, tout en rappelant que la capacité à fournir des garanties démocratiques (accessibilité et inclusivité des services, pluralité dans la prise de décision, confidentialité des données privées…) est aussi un facteur essentiel au succès de la gouvernance décentralisée sur le long terme.

7 Bribe Protocol: https://www.bribe.xyz/

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