MONNAIE ÉLECTRONIQUE PAIR-À-PAIR & ARGENT PROGRAMMABLE

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.

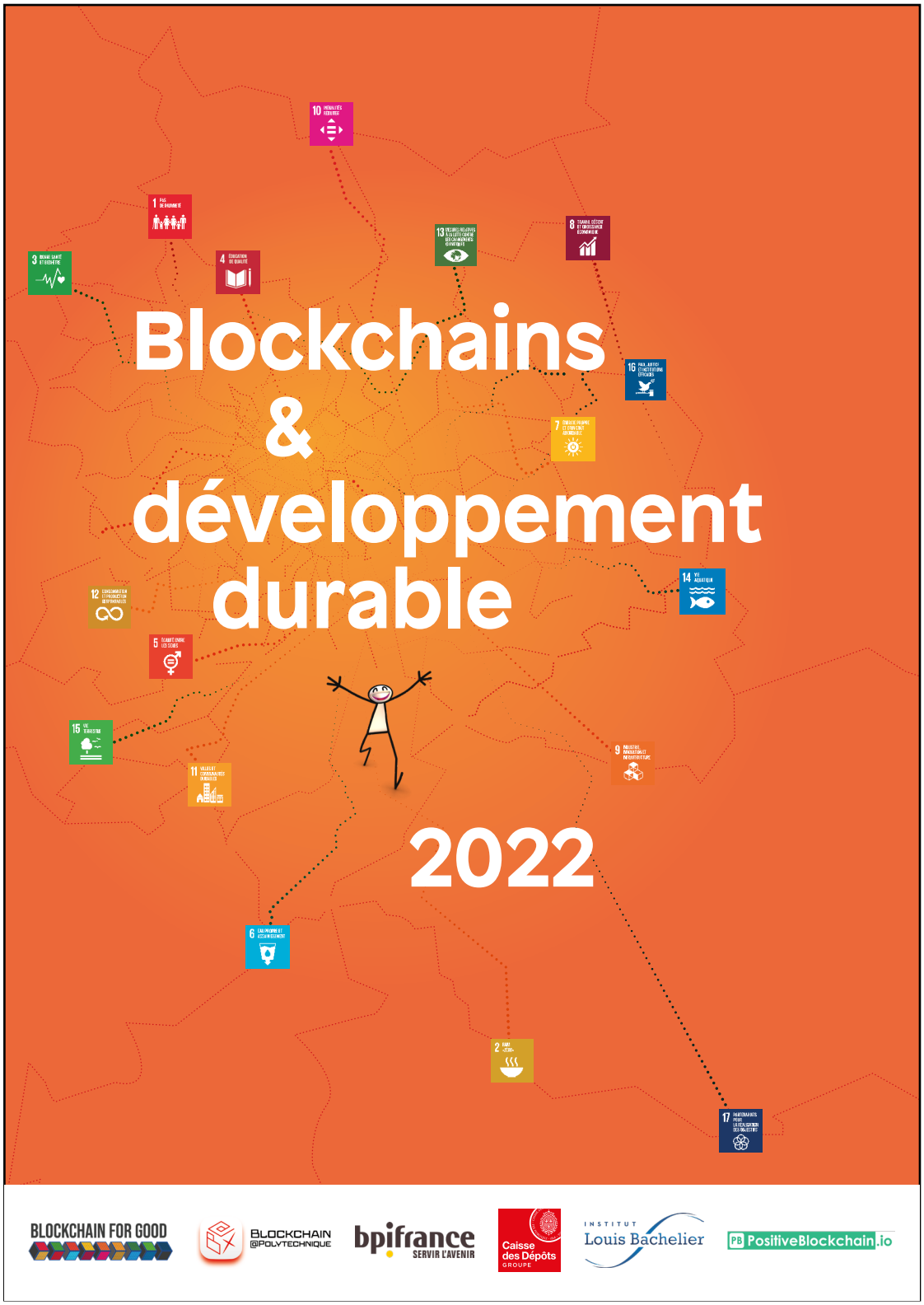
Bpifrance finance les entreprises - à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi leur activité export à travers une large gamme de produits. Conseil, université, 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 - MONNAIE ÉLECTRONIQUE P2P & ARGENT PROGRAMMABLE

Hervé Alexandre, Pierre Champsavoir, Martin Chazelle, Noémie Dié, Christophe Gbossou, Alejandro Gómez, Audran Gouis, Thibaud Huriez, Paul Pflimlin, Paul Rivière.

TABLE DES MATIÈRES

ENVOIS DE FONDS TRANSFRONTALIERS ---------- 10

PAIEMENT ET MICRO-PAIEMENT EN PAIR-À-PAIR ---------- 13

DEFI - EMPRUNTER, ÉPARGNER, INVESTIR ---------- 19

MONNAIES LOCALES COMPLÉMENTAIRES ---------- 23

ASSURANCES ---------- 25

REVENU UNIVERSEL ---------- 28

FINANCEMENT PARTICIPATIF ---------- 32

FINANCE INCLUSIVE ---------- 34

INVESTISSEMENT D'IMPACT ---------- 35

VÉRIFICATION D'IMPACT ---------- 36

PROJET EXEMPLAIRE : HIVEONLINE ---------- 41

ENJEUX ET QUESTIONS ---------- 44

GLOSSAIRE ---------- 46

ÉDITEUR ---------- 56

MONNAIE ELECTRONIQUE PAIR-A-PAIR ET ARGENT PROGRAMMABLE

Nombre de projets dans la base : 235

Nombre de projets actifs : 141

Nom des projets actifs : 0x ; AAVE ; Abra ; Acre Africa micro-insurance ; Adhara ; Airfox ; Akoin ; Akropolis ; Algorand ; Arbol ; Arcadia Blockchain Technologies ; B Protocol ; Bazaar Tech ; Bisq ; Bit Sika ; Bitpesa ; Bitt ; Bloom ; Botkeji (Kaoun) ; Bottlepay ; Cambiatus ; Cellulant ; CELO ; CentBee ; Centrifuge ; Chia ; Chynge ; Circles ; ClickPesa ; Coinify ; Coins.ph ; Colendi ; Compound ; Compound Labs ; Crowdforce ; Crypto Development Fund (CDF) ; Curve ; DEMARS ; Dether ; dGE - Diggi ; Dharma ; Diem (ex Libra) ; Digital Citizen Fund ; DistributedTown ; Dorium ; Eco Coin ; EcoChain ; efforce ; Ejara ; Etherisc ; Ethic Hub ; Evercity ; Everex ; Experty.io ; FintruX ; Flutterwave ; Freecoin ; FutureThinkers NFT ; Galoy ; Gooddollar ; Grassroots Economics ; Hive online ; Humaniq ; IcrowdU ; Impact Cred ; Inclusivity.network ; Insurwave ; Invictus Capital ; IOHK ; ixo foundation ; KamPay ; Kin ; Kivéclair ; Kiwi New Energy ; Korapay ; KYC-Chain ; Leman ; Local Bitcoin ; Lumoin ; MakerDAO ; M-Akiba ; Moeda ; Mojaloop ; MonedaPAR.com ; Money Track ; Muun ; Mybit ; Neco ; Nexo ; Oradian's Stellar integration ; Pancake Swap ; Parity.Tech ; Paxful ; PayCase ; Pesabase ; PledgeCamp ; Project Greshm ; Proof of Impact ; Qitmeer ; QLAY ; Raay ; Raise ; RAZ Finance ; REMIIT ; Remitano ; Retreeb ; Ricult ; Rupee Blockchain ; SALT ; Senditto ; sharehope ; Smart Valor ; SmartCredit ; SparkPoint ; Stellar ; Superfluid ; SureRemit ; Suretly ; Taro (protocol) ; Tecra ; Telcoin ; Tempo's Stellar integration ; Token Engineering Commons (TEC) ; Topl ; TrafiGuard (Bloom) ; Trustlines Network ; UCASH ; Uniswap ; Uphold ; Uulala ; VipiCash ; Vumi's Stellar Integration (Praekelt Foundation) ; Waba ; Weifund ; Women's coin ; Worldremit ; Wyre ; Xago ; Xend ; Yensesa ; Zlto ; *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/

Parce que Bitcoin est d'abord un « système de Monnaie Électronique en Pair-à-Pair[1] », le chapitre « Monnaie électronique pair-à-pair & argent programmable » est logiquement la catégorie dans laquelle nous avons recensé le plus de projets dans la base de données PositiveBlockchain.io.

Un système de paiement traditionnel est, selon la Banque des règlements internationaux (BRI), surnommée la « banque des banques centrales[2] », un « *système constitué d'un ensemble d'instruments, de procédures bancaires et de systèmes interbancaires de transfert de fonds, destiné à assurer la circulation de la monnaie* ». Alors qu'un système de monnaie électronique pair-à-pair est un protocole de réseau pair-à-pair, utilisant la cryptographie asymétrique et assorti d'un mécanisme de consensus afin de maintenir le registre des échanges de la monnaie électronique directement entre ses utilisateurs, sans plus passer par un organisme financier ou tiers de confiance.

« *Le problème fondamental de la monnaie conventionnelle est toute la confiance qui est nécessaire pour qu'elle fonctionne* », écrivait Satoshi Nakamoto avant de disparaître[3]. « *Il faut faire confiance à la banque centrale pour qu'elle ne dévalorise pas la monnaie, mais l'histoire des monnaies fiduciaires est pleine de violations de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer électroniquement, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction en réserve*[4] ».

Parmi les projets identifiés dans la base de données, bon nombre participent de ce mouvement initié en 2018 appelé Finance Décentralisée - DeFi, pour *Decentralized Finance* ou encore « Finance ouverte » - *Open Finance*, comme le suggère Clément Jeanneau de Blockchain Partner, pour marquer le fait que la Finance ouverte est d'abord un moyen et non une fin en soi. La DeFi permet 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**. Aujourd'hui, le système financier tel qu'il est conçu exclut l'ensemble de la population qui n'a pas d'identité[5] (voir Chapitre Identité et Propriété). Selon le Global Findex de la Banque mondiale[6], si 3,8 milliards de

1 « Bitcoin : un système de paiement électronique pair-à-pair », Satoshi Nakamoto, bitcoin.org, consulté le 10 mai 2022, https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf
2 La Banque des règlements internationaux (BRI, en anglais *Bank for International Settlements*, BIS) est une organisation financière internationale créée en 1930 réunissant 63 banques centrales dans le monde, dont l'activité équivaut à 95 % du PIB mondial.
3 « The Crypto-Currency Bitcoin and its mysterious inventor », Joshua Davis, October 3, 2011, https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
4 *Ibid.*
5 Voir Chapitre « Identité et propriété ».
6 Demirguc-Kunt, Asli; Klapper, Leora; Singer, Dorothe; Ansar, Saniya; Hess, Jake. 2018. « Base de données Global Findex 2017 : Mesurer l'inclusion financière et la révolution technico-financière ». Washington, DC

personnes dans le monde possèdent un compte auprès d'une banque ou d'un service d'argent mobile, 1,7 milliards de personnes n'y ont pas accès. La Finance décentralisée ne s'adresse pas directement aux plus défavorisés, mais permet à quiconque en a les moyens d'accéder à des produits financiers, avec ou sans identité régalienne, et indépendamment du pays où il se trouve.

De plus, cette monnaie électronique pair-à-pair ne se cantonne pas à concurrencer la monnaie traditionnelle en tant qu'instrument d'échange. Parce qu'elle est avant tout informatique, **cette monnaie électronique est également programmable, à travers les blockchains dites de deuxième génération (Ethereum, Tezos, Solana …)**. Des règles informatiques, que l'on appelle *smart contracts**[7], précisent quand et comment la valeur est échangée, renouvelant de fond en comble l'usage de la monnaie traditionnelle, tout en inventant des services financiers totalement inédits. L'inclusion financière portée par les monnaies électroniques pair-à-pair et l'argent programmable est au coeur de huit des dix-sept Objectifs de développement durables (ODD), qui en font une cible à part entière, l'ODD 1 sur l'élimination de la pauvreté ; l'ODD 2 sur l'élimination de la faim, la réalisation de la sécurité alimentaire et la promotion de l'agriculture durable ; l'ODD 3 sur la bonne santé et le bien-être ; l'ODD 5 sur l'égalité des sexes et l'autonomisation économique des femmes ; l'ODD 8 sur la promotion de la croissance économique et de l'emploi ; l'ODD 9 sur la promotion de l'industrialisation, de l'innovation et des infrastructures ; et l'ODD 10 sur la réduction des inégalités. Par ailleurs, l'ODD 17 sur le renforcement des moyens de mise en œuvre prévoit implicitement que l'inclusion financière jouera un rôle plus important en mobilisant davantage d'épargne pour favoriser l'investissement et la consommation, qui sont porteurs de croissance[8].

Comme nous le verrons, la diversité des applications des monnaies électroniques pair-à-pair n'a de limite que l'imagination de leurs concepteurs : Envoi de fonds en pair-à-pair (remittances) (**Bitcoin, Stellar, portefeuilles de crypto-devises**), paiement et micro-paiement en pair-à-pair (**Lighting Network/protocole Taro**, **Celo**, **Retreeb**), prêt et emprunt d'argent en pair-à-pair et Finance décentralisée (**Maker DAO** et **DAI**, **Compound**, **Aave**, **Uniswap**), évaluation du risque et notation de crédits (**FintruX**, **TrafiGuard**), monnaie dirigée et monnaie complémentaire décentralisée (**Leman**, **Grassroot Economics**, **Money Track**), assurance décentralisée reliée à un réseau d'oracles décentralisés (**Etherisc, Arbol**), revenu universel (**ImpactMarket**, **GoodDollar**), donation sans intermédiaire (**Kiveclair**), financement ou investissement participatif décentralisé (**Tecra Space, Raise**), inclusion financière (**Ethic Hub, Waba**, **Hive Online**), vérification d'impact (**Ixo Foundation, Proof of Impact**) ou encore investissement d'impact (**Sun Exchange)**.

- World Bank. openknowledge.worldbank.org License: CC BY 3.0 IGO.
7 Les mots marqués d'un astérisque font l'objet d'une définition dans le glossaire.
8 L'inclusion financière et les ODD, UNCDF, consulté le 10 mai 2022, https://www.uncdf.org/fr/financial-inclusion-and-the-sdgs

Envois de fonds transfrontaliers

En 2020, 200 millions de femmes et d'hommes, travailleurs migrants, ont envoyé l'équivalent de 544 milliards de dollars à plus de 800 millions de membres de leur famille estime l'ONU[9]. Les **envois de fonds individuels**, parfois d'une valeur relativement faible, **représentent pourtant collectivement des flux trois fois supérieurs à ceux de l'aide publique au développement mondiale**. Selon la Banque mondiale, en 2020, les transferts de fonds officiellement enregistrés[10] vers les pays à revenu faible et intermédiaire ont atteint 540 milliards de dollars, soit seulement 1,6 % de moins que les 548 milliards de dollars observés en 2019, et ce malgré la pandémie de Covid-19[11]. Quant aux transferts d'argent *via* mobile, bien que dérisoires par rapport à l'envoi traditionnel de fonds, ils s'élèvent à 16 milliards de dollars en 2022, en hausse de 48 % par rapport à l'année précédente[12].

Or ces fonds passent tous par des organismes financiers, qui ponctionnent une commission sur chaque envoi. La réduction du coût des transferts de fonds correspond à l'indicateur 10.c.1 des Objectifs de développement durable, qui fixe une cible de 3 % de frais. Néanmoins, ces derniers s'élèvent aujourd'hui en moyenne à 7,60 % du montant envoyé. Ces frais sont les moins élevés en Asie du Sud, à 4,9 %, et les plus élevés en Afrique Sub Saharienne, à 8,2 %[13].

Un transfert d'argent traditionnel par un opérateur financier ou un opérateur de télécommunication est ponctionné d'une commission calculée en pourcentage, passe par de nombreux intermédiaires et prend parfois plusieurs jours. Une transaction entre particuliers *via* une blockchain publique ne coûte que quelques centimes et est validée en quelques minutes, à l'instar du réseau **Stellar**, une infrastructure de paiement distribuée, libre d'utilisation et *open source*, fondée en 2014 par Joyce Kim et Jed McCaleb.

Ou encore le protocole Bitcoin sur le réseau *Lighting Network**, dont le principe consiste à ouvrir un canal de paiement au-dessus de la blockchain Bitcoin afin d'opérer des transactions à l'échelle de micro transactions, quasiment sans frais, en enregistrant seulement deux transactions sur la blockchain principale : celle qui ouvre et ferme le canal de transaction (voir encadré p.87).

9 Les envois de fonds, une bouée de sauvetage, Nations Unies, consulté le 10 mai 2022, https://www.un.org/fr/observances/remittances-day

10 Dilip Ratha, Eung Ju Kim, Sonia Plaza, and Ganesh Seshan. 2021. « Migration and Development Brief 34: Resilience: COVID-19 Crisis through a Migration Lens. » KNOMAD-World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO

11 « Defying Predictions, Remittance Flows Remain Strong During COVID-19 Crisis », World Bank, Press Release, May 12, 2021, https://www.worldbank.org/en/news/press-release/2021/05/12/defying-predictions-remittance-flows-remain-strong-during-covid-19-crisis

« State of the Industry Report on Mobile Money 2022 », GSMA. https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_French.pdf

13 Dilip Ratha, Eung Ju Kim, Sonia Plaza, and Ganesh Seshan. 2021. « Migration and Development Brief 34: Resilience: COVID-19 Crisis through a Migration Lens. » KNOMAD-World Bank, Washington, DC. License: Creative Commons Attribution CC BY 3.0 IGO

Selon la Banque mondiale, les commissions liées aux transferts d'argent traditionnels représentent un manque à gagner allant jusqu'à 16 milliards de dollars par an à ces travailleurs, en termes d'épargne pour celui qui envoie les fonds, ou en termes de fonds supplémentaires pour les destinataires.

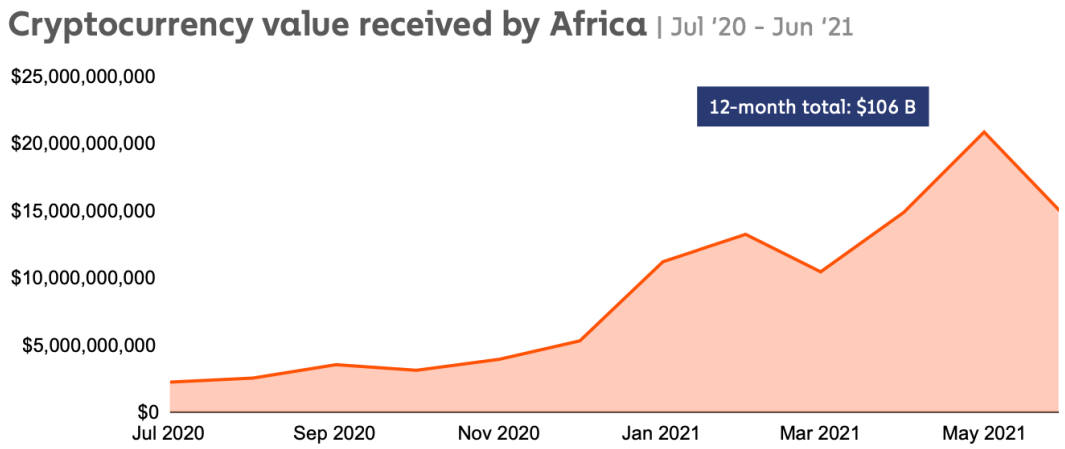
Au Salvador par exemple, 35 % de la population reçoit des transferts d'argent de l'étranger, à hauteur de 6 milliards de dollars en 2020, soit 23% de son PIB[14]. Dans des propos rapportés par CNBC, le Président du Salvador, Nayib Bukele estime que « *les prestataires de services monétaires comme Western Union et MoneyGram perdront 400 millions de dollars par an en commissions sur les envois de fonds, grâce à l'adoption du bitcoin par le pays*[15] ».

De plus, bon nombre de gouvernements de pays, notamment en Afrique, mettent en place une taxe sur les transactions *via* téléphone portable. Au Ghana par exemple, une taxe de 1,5 % sur l'argent mobile, connue sous le nom d'e-levy, suscite de fortes critiques et « *nuit à des millions de propriétaires de petites entreprises et à d'autres groupes à faible revenu, alors que le coût de la vie augmente*[16] ».

En marge des transferts de fonds par un intermédiaire bancaire ou un opérateur téléphonique, le transfert d'argent en pair-à-pair semble ainsi de plus en plus utilisé, notamment dans *plusieurs pays des marchés émergents, dont le Kenya, le Nigeria, le Vietnam et le Venezuela* explique le rapport *The 2021 Geography of Cryptocurrency Report*[17] édité par Chain Analysis.

Selon Shubham Pandey, rédacteur pour Ambcrypto, « *les restrictions sur les envois de fonds* [par les banques NDLR]*, couplées à l'inflation, ont été les principaux catalyseurs de la migration des personnes vers les crypto-actifs*[18] ». Au Nigeria par exemple, l'usage des cryptos actifs s'est développé après que la banque centrale du Niger ait interdit aux banques de détail de faciliter les transactions vers des crypto actifs, et qu'elle ait également limité par 500 dollars à la fois les envois de fonds à l'étranger de leurs clients[19].

14 « Money transfer to Venezuela, Remittance Flows Amidst Evolving Foreign Exchange », Manuel Orozco Kathryn Klaas, May 2020, thedialogue.org.
15 « El Salvador's new bitcoin plan could cost money providers like Western Union and others $400 million a year, says President Bukele », MacKenzie Sigalos, September 17, 2021, https://www.cnbc.com/2021/09/09/el-salvador-bitcoin-move-could-cost-western-union-400-million-a-year.html
16 « Africa's mobile money taxes may drive the poor out of the digital economy », Kent Mensah, Nita Bhalla, June 5, 2022, https://www.news24.com/citypress/business/africas-mobile-money-taxes-may-drive-the-poor-out-of-the-digital-economy-20220605
17 « The 2021 Geography of Cryptocurrency Report » Analysis of Geographic Trends in Cryptocurrency Adoption and Usage, Oct 2021, go.chainalysis.com.
18 « 'Smallest cryptocurrency economy,' Africa records 1200% hike in a year », Shubham Pandey, Sep 16, 2021, ambcrypto.com
19 Adedeji Owonibi : https://ng.linkedin.com/in/adedeji-owonibi- cité par Rapport Chainanalysis

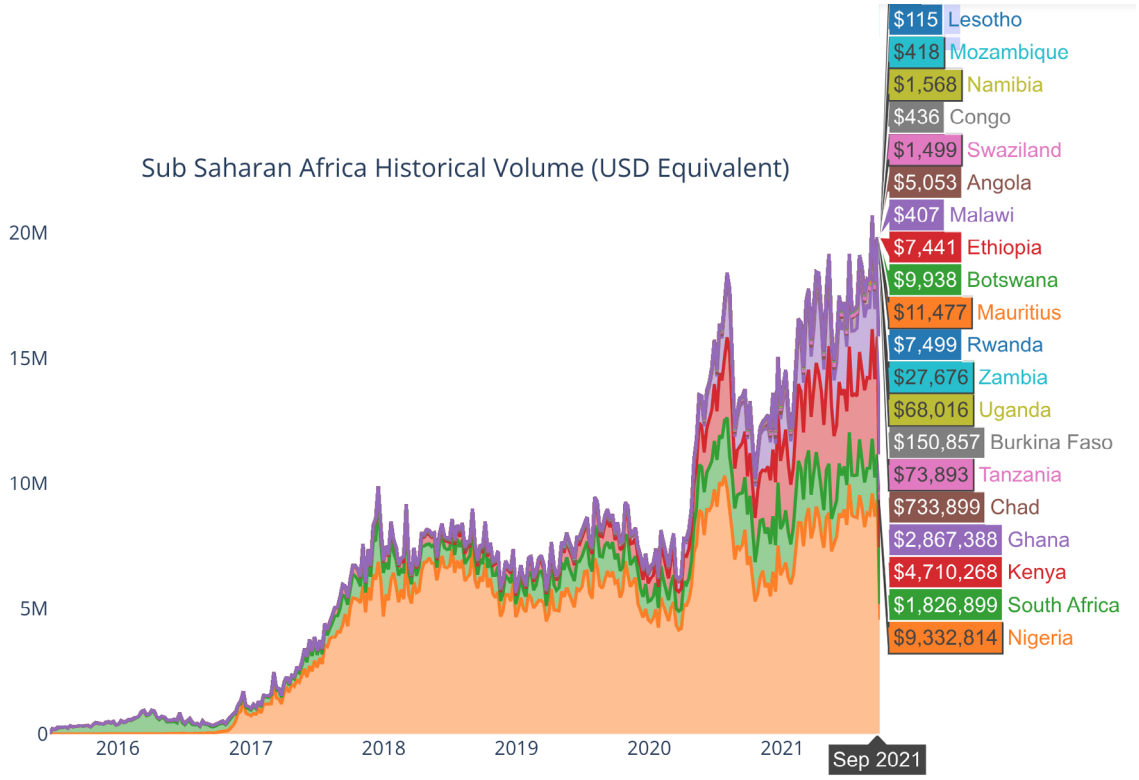


Order book trading volumes for Sub Saharan Africa from LocalBitcoins and Paxful in USD. Source : usefultulips.org - Septembre 2021.

Local Bitcoin, Paxful ou encore **Remitano** servent à acheter des Bitcoins ou autres crypto-actifs afin de les transférer sans banque, d'échapper à l'inflation et la dévaluation de la monnaie locale.

Créé en juin 2012 à Helsinki en Finlande, **LocalBitcoins**[20] permet aux utilisateurs d'échanger leur monnaie locale contre des bitcoins et offre une protection par séquestre afin de garantir la sécurité des crypto-actifs et des deux négociants. Sous la pression du Ministère de la Justice américain[21]LocalBitcoins a cessé, à partir de 2019, de permettre aux clients d'effectuer des échanges en face à face de crypto-actifs contre de l'argent liquide de manière anonyme. Avec presque cinq millions d'utilisateurs dans le monde, **Paxful**, fondée en 2015, est une place de marché d'échange pair-à-pair qui permet à ses utilisateurs d'acheter et vendre des crypto actifs *via* quelque 300 options de paiement. Artur Schaback, cofondateur de Paxful explique que les crypto actifs servent en Afrique pour faire du commerce avec l'étranger : « *Si vous travaillez avec un partenaire en Chine pour importer des marchandises à vendre au Nigeria ou au Kenya, il peut être difficile d'envoyer suffisamment de monnaie fiduciaire en Chine pour compléter vos achats (...) Il est souvent plus facile de simplement acheter des bitcoins localement sur un échange P2P, puis de les envoyer à votre partenaire.*» Créée en 2015, **Remitano** est basée aux Seychelles et propose un service similaire à celui de Paxful et LocalBitcoins. Remitano est particulièrement bien implanté au Vietnam, en Inde, au Cambodge ou encore au Nigéria. Comme le montre ce graphique publié sur usefultulip.org[22], le volume de

20 « A propos de Local Bitcoin », Local Bitcoin, consulté le 10 mai 2022, https://localbitcoins.com/about
21 « Local Bitcoinstops cash trades, personal offers on platform », Landon Manning, June 4, 2019, https://bitcoinmagazine.com/culture/localbitcoins-stops-cash-trades-personal-offers-on-platform
22 UsefulTulips.org est un site web qui explore les cas d'usage des crypto-actifs dans le monde. Les graphiques présentés sur le site Web proviennent des données d'échange des sites web d'échange de bitcoins en pair-à-



Sub Shaharan Africa Historical Volume (USD Equivalent)
Source : usefultulips.org - Septembre 2021.

transactions enregistrées sur LocalBitcoins et Paxful au Nigéria, en Afrique du Sud, au Kenya et au Ghana enregistre une forte hausse depuis le début de l'année 2021. L'usage de crypto-actifs pour se protéger de l'inflation a toutefois débuté dès 2013, lorsque des Chypriotes achetèrent des bitcoins pour préserver leur épargne.

Paiement et micro-paiement en pair-à-pair

L'une des critiques récurrentes à l'encontre des crypto-actifs est qu'ils ne seraient pas un moyen de paiement stable du fait de leur forte volatilité. Or la diversité des crypto-actifs et des initiatives de systèmes de paiement alternatifs contredit largement cette idée reçue. Non seulement des crypto-actifs peuvent servir de moyen de paiement, dont, pour certains, les frais sont bien moins élevés que les systèmes de paiement centralisés, mais permettent également de construire des services monétaires en pair-à-pair inédits, du fait de leur caractère programmable. Par exemple, le réseau **Bitcoin** permet d'effectuer des transactions en Satoshi sur un canal Lighting network*, de manière extrêmement rapide et quasiment sans frais. La blockchain **Celo** et ses crypto-actifs stables* indexés sur les

pair les plus populaires au monde, LocalBitcoins et Paxful. https://www.usefultulips.org/about.html

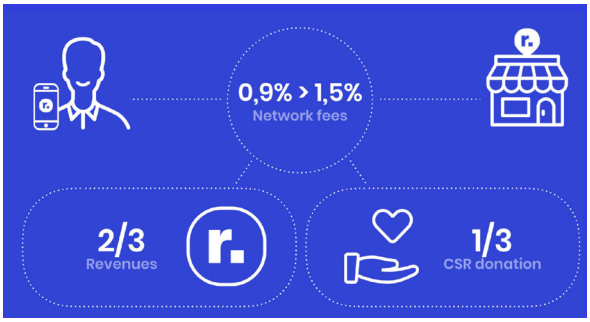
monnaies fiat* permettent d'effectuer des transactions en pair à pair dont les frais s'élèvent en général autour de 0,01 $. Le développement de *smart contracts** à partir d'une monnaie comme le cUSD inaugure des services inimaginables avec le système financier actuel.

Retreeb se présente comme un moyen de paiement éthique, en affectant un tiers de sa commission à des projets sociaux et environnementaux. A mi-chemin entre un nouveau moyen de paiement et un système décentralisé de financement participatif, **Retreeb** se présente comme une alternative aux systèmes de paiement centralisés comme Visa, Mastercard, Stripe ou Paypal « *en plaçant la responsabilité sociale et environnementale (RSE) au cœur de son modèle économique*[23] ». Fondée en 2019 à Genève en Suisse par Jérémi Lepetit et Sayah El Yatim, l'entreprise se définit comme un moyen de paiement éthique pour le grand public et comme une réponse à la question de savoir « *comment capter la valeur produite par les transactions de paiement, pour mieux la réaffecter aux enjeux sociétaux de notre époque ?*[24] » explique Jérémi Lepetit.

Comme tout moyen de paiement, Retreeb s'adresse au consommateur final qui paye un commerçant à l'aide d'une application téléchargée sur son smartphone ou via une carte bancaire biométrique. Le paiement en monnaie fiat est converti en un token indexé[25] à la monnaie fiat de manière transparente pour l'utilisateur (euro, franc suisse etc.). Jérémi Lepetit, co-fondateur et CEO de Retreeb explique ainsi que « *le stableTreeb est collatéralisé à 100 % par la réserve en monnaie FIAT correspondante au dépôt. Le stableTreeb est* mint [créé] *au dépôt et* burn [détruit] *après le paiement en monnaie FIAT du commerçant toutes les 72h00 maximum. Le stableTreeb évolue en vase clos dans notre système. Il n'est listé nulle part. Ces propriétés garantissent sont indexation 1:1 permanente. D'un point de vue juridique ce n'est pas un stablecoin mais une monnaie électronique* on-chain* ». L'intérêt pour le commerçant est de sensiblement baisser la commission bancaire traditionnelle, de l'ordre de 2,5 à 5 %, payée aux infrastructures de paiement centralisées comme Visa ou Paypal, à une commission ramenée entre 0,9 % et 1,5 %.

Le paiement déclenche un *smart contract* appelé « contrat social autonome » (*Social Smart Contract*) qui implique, en plus de celui qui paye et celui qui encaisse, une tierce partie : le bénéficiaire social, (*Social Beneficiary*) représentant une cause, une association, une Organisation non gouvernementale, ou un projet désigné comme bénéficiaire des engagements sociétaux, choisi par l'utilisateur.

23 Retreeb - Pitchdeck, consulté le 28 avril 2022, https://retreeb.io/assets/retreeb-pitchdeck.pdf
24 « Cette finance qui veut changer le monde », Myret Zaki, 16 novembre 2020, https://www.bilan.ch/finance/cette-nance-qui-veut-changer-le-monde
25 Selon Jérémi Lepetit, cofondateur de Retreeb, « Le stableTreeb est collatéralisé à 100% par la réserve FIAT correspondante au dépôt. Il est *mint* [créé] au dépôt et *burn* [détruit] après le paiement en FIAT du commerçant toutes les 72h maximum. Le stableTreeb évolue en vase clos dans notre système. Il n'est listé nulle part. Ces propriétés garantissent sont indexation 1:1 permanente. D'un point de vue juridique ce n'est pas un stablecoin mais une monnaie électronique *on-chain** ». Entretien Association Blockchain for Good, 30 juin 2022.



Source : https://retreeb.io/

Le protocole de paiement développé par Retreeb, Cell, est construit sur un *fork** du Directed Acyclic Graph (DAG[26]) de Lachesis développé par la Fondation Fantom[27]. Le mécanisme de consensus qui permet de valider et sécuriser les transactions, Lachesis aBFT (asynchronous Byzantine Fault Tolerant), a été utilisé pour notamment réduire les commissions financières, reposer sur une infrastructure financière capable de supporter jusqu'à 10 000 transactions par seconde tout en étant interopérable avec la Ethereum Virtual Machine (EVM)*, et enfin, pour minimiser les coûts environnementaux et l'impact carbone du système de paiement.

Retreeb met en œuvre deux tokens :

- Le(s) Treeb, un crypto-actif stable* collatéralisé sur la monnaie de l'utilisateur et soutenu par une réserve de valeur strictement égale à son offre ce qui permet à l'utilisateur, indépendamment de la monnaie fiat qu'il utilise, de ne pas avoir à se soucier de la conversion. Ainsi, un sTreeb en France équivaut à un euro, 1 sTreeb en Suisse équivaut à un franc suisse, un sTreeb en Angleterre équivaut à un pound etc. « *Le système permet de construire un sTreeb par zone monétaire qui aura toujours la valeur de la devise locale de l'utilisateur* » détaille Jérémi Lepetit.
- Et le (u)Treeb ou TREEB, un jeton utilitaire de gouvernance utilisé par la communauté Retreeb à des fins de gouvernance, notamment pour sélectionner les projets RSE supportés, et pour accéder à un statut *premium* dont l'objectif est d'encourager la propriété à long terme des (u)Treeb par ses utilisateurs.

Celo imaginé en 2017 et lancé en mai 2020 à San Francisco aux Etats-Unis, permet à quiconque possédant un smartphone d'envoyer et recevoir des crypto-actifs et s'adresse tout particulièrement aux populations qui sont exclues du système bancaire traditionnel. Celo a longtemps été considéré comme le concurrent le plus sérieux du projet de crypto-actif Libra, lancé par Facebook début 2020, rebaptisée Diem, puis finalement arrêté.

Si les velléités de Facebook étaient de lancer une monnaie mondiale privée, Celo est l'équivalent *a contrario*, *open source*[28] et accessible à tous.

26 « Qu'est-ce qu'un graphe orienté acyclique (DAG) dans le domaine des crypto-actifs ? », Binance Academy, July 19, 2020, https://academy.binance.com/fr/articles/what-is-a-directed-acyclic-graph-dag-in-cryptocurrency
27 « What is Fantom ? », Fantom, retrieved May 10, 2022, https://fantom.foundation/fantom-faq/
28 Celo Gituhb: https://github.com/celo-org/celo-blockchain

C'est une blockchain publique sans permission issue d'un *fork** de la blockchain Ethereum. Outre son jeton natif, qui permet d'opérer la gouvernance décentralisée du protocole, Celo a développé trois crypto-actifs stables* : le Celo Dollars (cUSD), le Celo Euro (cEUR), le Celoa Real (cREAL), chacun indexé au dollar américain, à l'euro, et au real brésilien, et dont la circulation s'établit, en mai 2022, à 72 millions de cUSD, 37 millions de cEUR et 9 millions de cREAL. La promesse de Celo est donc d'être « *une blockchain* mobile-first *qui rend les outils et services financiers décentralisés (DeFi) accessibles à toute personne possédant un téléphone portable* ». Le portefeuille Celo (et les 26 autres compatibles) permet non seulement à ses utilisateurs d'effectuer et recevoir des paiements directement aux personnes figurant dans la liste de ses contacts, mais également, de payer les commerçants qui l'acceptent, d'envoyer des fonds transfrontaliers pour de très faibles coûts, d'envoyer et de recevoir une aide caritative ainsi que de nombreux services « crypto » développés à partir de l'écosystème Celo.

A l'instar d'Ethereum, Celo est programmable à travers des *smart contracts** utilisant la machine virtuelle Ethereum* (EVM). Celo repose cependant sur un algorithme de consensus basé sur la preuve d'enjeu appelé Tolérance de panne byzantine pratique* (pBFT) plutôt que sur la preuve de travail, ne requérant donc pas de dépense énergétique pour valider et sécuriser les transactions. Les crypto-actifs développés sous Celo sont conformes à la norme Ethereum ERC-20 et donc compatibles avec tous les outils et applications de l'écosystème d'Ethereum.

Les numéros de téléphone sont associés à des adresses, au nombre de 2,8 millions en mai 2022, à l'aide d'un protocole d'identité décentralisé* (voir Chapitre identité et propriété). La couche logicielle de Celo a été développée pour être compatible avec tous les smartphones, y compris ceux qui ont peu de mémoire et une faible connectivité au réseau. De plus, plutôt que de stocker l'intégralité des transactions de la blockchain sur le téléphone de chacun, Celo a développé un système basé sur zk-SNARK[29] permettant aux nœuds mobiles de se synchroniser avec la blockchain Celo en utilisant des preuves à divulgation nulle de connaissance* (ZKP), ce qui permet de vérifier rapidement le calcul de synchronisation de la blockchain sans avoir à l'exécuter localement et d'assurer une confidentialité des données.

Depuis son lancement en mai 2020, la blockchain Celo a levé 66,5 millions de dollars en huit tours de table[30]. Du fait de sa compatibilité avec le réseau Ethereum, Celo est utilisé par plusieurs centaines de projets blockchain et d'applications

29 « Techniques cryptographiques visant à assurer la confidentialité des données sur une blockchain publique . Source : « Les zk-SNARKs et les zk-STARKs expliqués », February 26, 2019, https://academy.binance.com/fr/articles/zk-snarks-and-zk-starks-explained

30 « Celo », Crunch Base, Crunch Base website, retrieved May 10 2022, https://www.crunchbase.com/organization/celo-3846

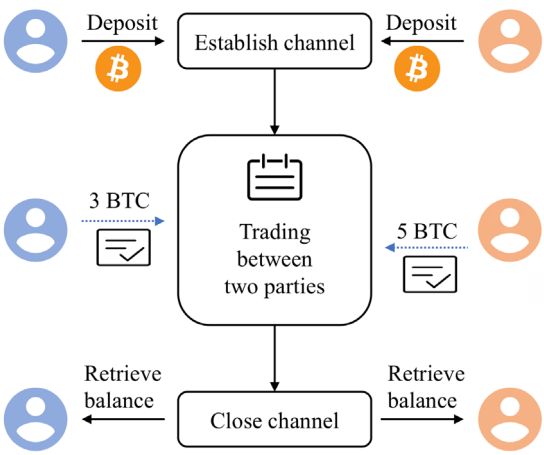


Figure 1

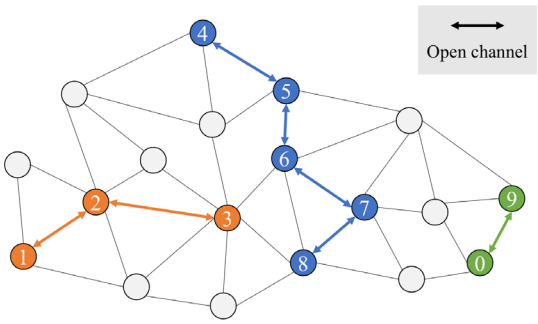


Figure 2

Processus du Lightning Network
Source : Zhou, Qiheng & Huang, Huawei & Zheng, Zibin. (2020). Solutions to Scalability of Blockchain: A Survey. IEEE Access. PP. 10.1109/ACCESS.2020.2967218.

décentralisées partout dans le monde[31]: **Impact Market** et **GoodDollar**, qui collectent des dons redistribués sous la forme d'un revenu de base à destination de populations défavorisées, **Toucan Protocol**, **Wren** et **Moss** qui permettent de compenser son empreinte carbone, **Grameen**, une application d'aide humanitaire ou encore **Masa,** un protocole de crédit décentralisé, pour n'en citer que quelques-uns.

Contrairement à une idée reçue, la blockchain Bitcoin permet également d'effectuer des micro transactions pour un coût proche de zéro. Le réseau Lightning (*Lightning Network*), un protocole de paiement de pair-à-pair construit comme une application de deuxième couche sur la blockchain Bitcoin, permet d'opérer des transactions en bitcoin extrêmement rapides, de l'ordre d'un million par seconde, quasiment sans frais et sans dépense énergétique[32], 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 montée en charge (scalabilité) de Bitcoin qui, pour rappel, ne peut traiter que 7 à 10 transactions par seconde. Le réseau Lightning fonctionne depuis mai 2018.

31 « Apps », Celohub, Celohub website, retrieved May 10, 2022, https://celohub.org/apps
32 «Comprendre le Lightning Network»,Yorick de Mombynes, Institut Sapiens, 23 juin 2020, https://www.institutsapiens.fr/wp-content/uploads/2020/06/Comprendre-le-Lightning-network.pdf

Le livre blanc[33] du réseau Lightning, rédigé par Joseph Poon et Thaddeus Dryja de Lightning Labs et publié le 14 janvier 2016, le décrit comme « *un réseau de canaux de paiement dans lequel chacun des hôtes est connecté en pair-à-pair, et sans recours à une hiérarchie centrale, forme une structure de réseau maillé où chaque nœud peut recevoir, envoyer et relayer des transactions* ».

Sur la figure 1 (voir *supra*), qui se lit de haut en bas, deux personnes disposant d'un portefeuille bitcoin établissent un canal de paiement au-dessus de la blockchain Bitcoin (hors chaîne) en déposant chacun un certain montant. Ils pourront ensuite, à travers ce canal de paiement, effectuer autant de transactions qu'ils le souhaitent (toujours d'un montant inférieur à la somme initiale déposée), validées instantanément, à des frais proches de zéro. Lorsqu'ils le souhaitent, ces deux personnes pourront fermer le canal, ce qui aura pour effet d'enregistrer le solde final de leur compte respectif sur la blockchain Bitcoin. Il n'y aura donc eu d'enregistrées dans la blockchain Bitcoin que la transaction initiale et celle finale, et autant de transactions que souhaitées, 100, un million ou plus, traitées au sein du même canal de paiement.

De plus, le réseau Lightning met en œuvre un réseau de canaux de paiement, comme indiqué en figure 2, pour effectuer des transactions hors-chaîne (*off chain**) entre deux parties qui n'ont pas de canal de paiement direct établi entre elles mais qu'une route relie, de telle sorte que, le nœud 1 et 3 ou 4 et 8 peuvent également effectuer des transactions en pair-à-pair.

En avril 2022, le Lightning Labs a annoncé le lancement du **protocole Taro**, qui vise à pouvoir utiliser des crypto-actifs stables* dans les applications présentes sur le réseau Lightning[34]. Elizabeth Stark, cofondatrice et CEO de Lightning Labs explique ainsi que Taro va *« bitcoiniser le dollar ».* Le protocole Taro permet de convertir des crypto-actifs stables* indexés au dollar en bitcoin, les router à travers le réseau Lightning, puis les convertir à nouveau de bitcoin en crypto-actifs stables* indexés au dollar, ce qui permettra, selon Elizabeth Stark, « *de mettre Bitcoin à la portée de milliards de personnes*[35] ».

L'intérêt d'utiliser le réseau Lightning est qu'il n'y a quasiment pas de limite au nombre de transactions par seconde sur le réseau, les transactions sont instantanées d'un bout à l'autre du monde et les frais de transaction sont potentiellement inférieurs à un Satoshi (0,00000001 BTC, soit 0.000039 $ en avril 2022). Au 1er juin 2022, le Lightning Network compte 17 570 nœuds et 85 320 canaux à travers lesquels

33 « The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments », Thaddeus Dryja & Joseph Poon, Lightning Network Website, January 14, 2016, https://lightning.network/lightning-network-paper.pdf
34 « Announcing Taro: A New Protocol for Multi-Asset Bitcoin and Lightning », Ryan Gentry, April 5, 2022, https://lightning.engineering/posts/2022-4-5-taro-launch/
35 « Number of People Go Up, or Bitcoin as the World's Protocol of Value », Elizabeth Stark, April 5, 2022, https://medium.com/@lightning_labs/number-of-people-go-up-or-bitcoin-as-the-worlds-protocol-of-value-d1df7cefca37

circulent 3 920 BTC, soit 125 millions de dollars[36].

Kiveclair, [que nous présentons au chapitre Aide, Charité et Philanthropie – donation sans intermédiaire], donne à voir un cas d'usage intéressant du réseau Lightning. Débuté en octobre 2021 près de la ville de Goma, dans l'Est de la République démocratique du Congo (RDC), après l'éruption du volcan Nyiragongo, le projet Kiveclair, porté par une petite équipe sur place, avec le soutien technique et logistique du Cercle du Coin, Indenodes, Nodl et JohnOnchain, a pour objectif « *de venir en aide à une cinquantaine de familles en satoshi et les former à l'utilisation de Bitcoin* ». Il s'agit d'une campagne de dons en ligne, en satoshis* ou en Bitcoin, permettant d'équiper les personnes, sinistrées suite à l'éruption volcanique, d'un téléphone portable sur lequel est installé un portefeuille Bitcoin sur le réseau Lightning, à partir duquel chacun recevra deux fois par mois, pendant six mois, un don d'environ 25 USD en satoshis*. Les bénéficiaires participent également à une formation pour apprendre à utiliser ce portefeuille. Les bitcoins/Satoshis ne seront pas convertibles en monnaie locale, l'idée étant de les faire circuler dans l'économie locale à travers des commerces également accompagnés par Kiveclair, acceptant les paiements en bitcoin.

Selon Yorick de Mombynes, « *le nombre de participants, de canaux et de bitcoins engagés sur le réseau Lightning augmente de manière exponentielle depuis le début de l'année 2021*[37] » et devrait compter, selon les estimations d'un rapport publié par Arcane Crypto en octobre 2021, 700 millions d'utilisateurs d'ici 2030[38].

DeFi - emprunter, épargner, investir

Même si le terme DeFi, - pour Decentralized Finance, Finance Décentralisée, a été employé pour la première fois en août 2018 sur un chat Telegram entre des développeurs informatiques d'Ethereum et des entrepreneurs de Set Protocol, 0x et Dharma[39], la Finance Décentralisée est née avec Maker DAO, créée en 2014 par l'entrepreneur danois Rune Christensen, une organisation autonome décentralisée* (DAO* - *Decentralized Autonomous Organization*) construite sur la blockchain publique Ethereum. Ce nouveau système informatique, décentralisé, adresse le premier des problèmes du système monétaire et du système financier international : son accessibilité. Comme le note l'Association française pour le Développement des Actifs Numériques (ADAN), « *notre accès aux services financiers dépend bien souvent de notre classe sociale ou de notre localisation géographique. Pourtant, l'inclusion financière est synonyme d'inclusion sociale* ».

36 Lightning Network Search and Analysis Engine, retrieved June 1, 2022, https://1ml.com
37 « L'ingéniosité et l'inventivité du Lightning Network sont stupéfiantes », Rémy Demichelis, lesechos.fr, 25 août 2021. https://investir.lesechos.fr/marches/bitcoin-crypto-actifs/l-expert-l-ingeniosite-et-l-inventivite-du-lightning-network-sont-stupefiantes-1977196.php
38 « The State of Lightning », Arcane Research, October 5, 2021, https://arcane.no/research/reports/the-state-of-lightning
39 « What Is Decentralized Finance ?: A Deep Dive by The Defiant », Camila Russo, May, 2021, https://coinmarketcap.com/alexandria/article/what-is-decentralized-finance

Selon le site ethereum.org[40], la Finance décentralisée (DeFi) est « *une alternative globale et ouverte au système financier actuel - Des produits qui vous permettent d'emprunter, d'épargner, d'investir, de commercer, et plus encore - basés sur une technologie* open-source *avec laquelle tout le monde peut programmer* ».

Prenons l'exemple de Maker DAO pour mieux saisir les enjeux de la Finance décentralisée. Débutée en 2014 par Rune Christensen, et concrétisée en 2018 sous la forme d'une fondation dont le livre blanc a été publié en 2019[41], Maker DAO est une Organisation autonome décentralisée (DAO*) sur Ethereum mettant en œuvre deux jetons : le DAI et le MKR. Le jeton DAI, est un crypto-actif stable*, c'est à dire qui vise à maintenir sa valeur aussi proche que possible d'un dollar américain (USD) grâce à un système automatisé de *smart contracts** programmés sur la blockchain publique Ethereum. **Le service permet ainsi à des prêteurs et des emprunteurs en DAI d'opérer, via un ensemble de** *smart contracts***, les processus de prêt, de remboursement et de liquidation**.

Quant à l'Organisation autonome décentralisée*, elle rassemble les propriétaires de son token de gouvernance, le MKR, également programmé sur la blockchain publique Ethereum, et permettant à chacun de voter à propos de l'évolution du code informatique des *smart contracts**. Maker DAO se définit comme « *une monnaie stable et décentralisée qui ne fait aucune discrimination. Tout individu ou entreprise peut bénéficier des avantages de la monnaie numérique* ». En 2021, plus de 400 applications et services ont intégré le DAI comme monnaie électronique. En octobre 2020, alors qu'un milliard de DAI ont déjà été créés, la Maker Fondation explique que le service le plus utilisé est le placement en vue de lutter contre l'inflation, suivi des produits et services de la DeFi, puis les jeux, l'art digital et le e-commerce.

En mai 2022, ce sont dorénavant 9,6 milliards de DAI générés, pour une valeur totale bloquée de 12,6 milliards de dollars. « *De nombreux adeptes précoces des crypto-actifs ont été incités à explorer cette technologie en raison des turbulences économiques que connaissait leur pays* » explique la Fondation Maker DAO. S'il est impossible pour ces populations d'accéder aux monnaies fiat euros, dollars, yuan… le DAI s'achète quant à lui sur une plateforme d'échanges décentralisés (DEX*), accessible à partir d'un smartphone. Le DAI se serait particulièrement bien implanté en Amérique latine dont les pays sont soumis à une forte volatilité. En 2020, il aurait dépassé le Bitcoin en termes de volumes d'échange, notamment en Argentine, au Brésil, en Colombie et au Venezuela[42].

40 Ethereum.org est une ressource publique et *open source* pour la communauté Ethereum, à laquelle n'importe qui peut contribuer. L'Ethereum Foundation finance une petite équipe dédiée au développement et à la maintenance du site https://ethereum.org/fr/about/
41 DAO Maker - Whitepaper, 2019 https://drive.google.com/file/d/1tPRMktnros6ifJLfvQkrT6mAmEJvUufT/view
42 « The Top Five Ways the Dai Stablecoin Is Used Around the World » MakerDAO, MakerDAO website, Oct 23 2020 https://blog.makerdao.com/the-top-five-ways-the-dai-stablecoin-is-used-around-the-world/

En juillet 2021, la Maker Foundation a déclaré cesser ses opérations d'ici la fin de l'année et basculer vers une décentralisation totale, c'est à dire que la gouvernance sera entre les seules mains des membres de l'Organisation autonome décentralisée[43], représentée par ceux qui possèdent des tokens MKR. Maker DAO, ouvert à tous, attire même les banques, comme la Société Générale qui a testé un emprunt de 20 millions de dollars en octobre 2021[44].

Cette Finance ouverte se développe depuis 2018, en parallèle du système financier actuel, duquel il se distingue fondamentalement selon trois caractéristiques : « *il est nativement numérique ; il fonctionne sur des infrastructures décentralisées ; il est ouvert à tous, aussi bien en termes d'usage, de consultation que de participation à sa construction* » explique Clément Jeanneau. Selon l'agrégateur de données DefiLlama[45], la valeur totale verrouillée dans la DeFi atteindrait 245 milliards de dollars en décembre 2021, dont 163 milliards de dollars uniquement sur la blockchain Ethereum, suivi, dans l'ordre, par les blockchains publiques Binance Smart Chain, Terra, Avalanche, Solana, Tron, Fantom, Polygon, Arbitrum et DefiChain.

En juin 2022, la valeur totale verrouillée dans la Defi est tombée à 74 milliards de dollars.

La DeFi permet à quiconque en a les moyens, y compris ceux qui n'ont pas accès aux prêts classiques, de partout dans le monde, 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*. Parmi les applications phares de la DeFi, les plateformes d'échanges décentralisées (DEX*) et les protocoles de prêt et d'emprunt rencontrent le plus de succès. Les bourses d'échanges décentralisés, Decentralized Exchange, appelées DEX, permettent d'échanger des crypto-devises sans aucun intermédiaire, ou plateforme centralisée (Centralized Exchange Platform - CEX).

Uniswap, lancée en novembre 2018, est la première DEX, permettant à ses utilisateurs, à partir d'un simple portefeuille, d'échanger des jetons ERC20 basés sur le réseau Ethereum, tout comme PancakeSwap, une bourse d'échanges décentralisés de jetons BEP20, basée sur la Binance Smart Chain ou encore Curve Finance, fondée en 2020, une autre DEX* construite sur le réseau Ethereum, permettant d'échanger des crypto-actifs stables* à des frais réduits en utilisant notamment un protocole de teneur de marché automatisé (AMM[46]).

43 « MakerDAO Moves to Full Decentralization; Maker Foundation to Close in 'Months' The move by the protocol's home office has been long expected », Brady Dale, July 20, 2021, https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months/
44 « Société Générale Applies for $20M MakerDAO Loan Using Bond Token Collateral One of the largest banks in France is working with one of the largest protocols in DeFi on a historic step toward institutional adoption », Andrew Thurman, October 1, 2021, https://www.coindesk.com/business/2021/09/30/societe-generale-applies-for-20m-makerdao-loan-using-bond-token-collateral/
45 Defi Llama: defillama.com
46 Un teneur de marché automatisé (AMM) est un type de protocole d'échange décentralisé (DEX) qui s'appuie

Quant aux protocoles de prêt et d'emprunt comme **Nexo**, **Aave** ou encore **Compound**, tous trois créés en 2017, ce sont des protocoles *open source* qui permettent à leurs utilisateurs de placer et gagner des intérêts sur leurs crypto-actifs, en les déposant dans un des *pools de liquidité** pris en charge par la plateforme ou d'emprunter des crypto-actifs en déposant un collatéral souvent aussi, voire plus élevé que la somme empruntée. Il est possible d'y déposer de très nombreux crypto-actifs, dont le DAI de Maker DAO, précédemment cité.

Une autre offre de la DeFi s'adresse spécifiquement aux petites et moyennes entreprises, comme **FintruX**, créé à Singapour en 2017 ou encore **TrafiGuard** en 2020, construit sur la plateforme **Bloom**[47] de **0x**[48], un protocole *open source* qui permet l'échange d'actifs de pair-à-pair sur la blockchain Ethereum. Cette offre s'inscrit dans l'Objectif de développement durable 9, et tout particulièrement la cible 9.3, « *accroître, en particulier dans les pays en développement, l'accès des entreprises, notamment des petites entreprises industrielles, aux services financiers, y compris aux prêts consentis à des conditions abordables, et leur intégration dans les chaînes de valeur et sur les marchés*[49] ».

Bloom se présente comme « *un protocole de bout en bout d'attestation d'identité, d'évaluation des risques et de notation de crédit construit sur la blockchain Ethereum. Bloom permet aux prêteurs traditionnels et aux prêteurs en monnaie numérique de servir des milliards de personnes qui ne peuvent actuellement pas obtenir un compte bancaire ou une cote de crédit*[50] ». TrafiGuard, en s'appuyant sur Bloom, souhaite lancer une « *solution de financement du commerce pour les micro et petites entreprises*[51] » en réunissant de manière inédite acheteurs et vendeurs internationaux.

TrafiGuard permet à l'acheteur / importateur de déposer des fonds dans un *smart contract** créé sur Bloom. Ces fonds, déposés en crypto-actif stable* USDC (indexé sur un dollar) sont bloqués dans un *smart contract** qui génère des intérêts, et permet au vendeur/exportateur de contracter, sur place, un prêt dans sa monnaie locale. Pour prouver sa solvabilité, le vendeur/exportateur s'identifie sur **Bloom**, fournit des documents d'imposition locale, fournit la lettre de transport

sur un algorithme de tarification pour évaluer les actifs. Un AMM fonctionne de manière similaire à un échange de carnet d'ordres en établissant des paires de négociation - par exemple, BTC/DAI excepté que, les échanges se faisant de manière décentralisée, le donneur d'ordre interagit avec un *smart contract* dont la liquidité provient d'autres utilisateurs appelés fournisseurs de liquidité (LP).

47 « The Truth Platform », Bloom, retrieved May 10, 2022, https://bloom.co/

48 « Introduction to Ox », Ox, retrieved May 10, 2022, https://0x.org/docs/core-concepts

49 Objectif de développement durable 9 : « Accès de toutes les entreprises aux services financiers ». https://www.agenda-2030.fr/17-objectifs-de-developpement-durable/article/odd9-mettre-en-place-une-infrastructure-resiliente-promouvoir-une

50 « What is Bloom ? », Bloom, retrieved May 10, 2022, https://faq.bloom.co/article/5-what-is-bloom

51 « How TrafiGuard uses Bloom to Provide SME Financing on the Blockchain », David Raphael, March 17, 2021, https://bloom.co/blog/how-trafiguard-uses-bloom-to-provide-sme-financing-on-the-blockchain/

(*Bill of Lading*), c'est à dire le document légal délivré par un transporteur à un expéditeur qui détaille le type, la quantité et la destination des marchandises transportées et enfin, des informations vérifiables liées au transport international.

En fonction du score de risque calculé par Bloom, le vendeur/exportateur pourra contracter un prêt compris entre 10 % et 50 % de la garantie déposée par l'acheteur/importateur. Toutes les preuves de documentation sont fournies au *smart contract** *via* les réseaux d'oracles décentralisés de Chainlink. Les protocoles blockchain imbriqués sont donc celui de **Bloom**, qui permet de déployer les *smart contracts**, l'oracle **Chainlink**, pour certifier des données externes, le service de prêt et d'emprunt **Compound** (voir *supra*) et le crypto-actif stable* USDC pour assurer les échanges financiers transfrontaliers. Si le processus paraît complexe à première vue, il constitue cependant l'opportunité pour un vendeur/exportateur d'accéder à une solution de financement innovante à laquelle il n'aura jamais accès avec le système financier traditionnel.

Monnaies locales complémentaires

Une monnaie locale complémentaire est une monnaie créée en complément d'une monnaie nationale, afin d'être échangée dans une zone géographique déterminée pour notamment « *améliorer les échanges au niveau local et dynamiser l'économie réelle*[52] ». Dans les pays développés, les monnaies locales complémentaires sont un outil monétaire permettant de stimuler une économie responsable d'un point de vue social et environnemental, en relocalisant les approvisionnements à travers des circuits courts, et en stimulant les pratiques durables dans les entreprises et chez les particuliers[53]. Il existe peu de « crypto actif local » même si des initiatives similaires, au contexte réglementaire bien différent, ont eu lieu notamment au Kenya avec Grassroot Economics ou en Suisse avec le Léman[54]. Dans les pays en développement, quand la monnaie nationale se fait rare parce que l'économie d'un pays se contracte, les gens les plus défavorisés n'ont plus les moyens d'échanger des biens et services entre eux.

Depuis 2010, **Grassroots Economics** a mis en œuvre des programmes de monnaies communautaires inclusives (*Community Inclusion Currency* - CIC) dans plus de 45 localités au Kenya et a aidé au déploiement de deux monnaies communautaires en Afrique du Sud et au Congo, et accompagne plusieurs projets en dehors de l'Afrique.

52 Monnaie locale complémentaire : https://www.novethic.fr/lexique/detail/mlc.html
53 « Le numérique au secours des monnaies locales et complémentaires », Bénédicte Martin, Netcom, journals.openedition.org, 18 décembre 2018, consulté le 15 décembre 2021.
54 « Le Léman, concrètement ? », Monnaie Leman, https://monnaie-leman.org/le-leman-concretement

Elle a également formé des gens au *design* de monnaie communautaire en Colombie, au Nigéria et en France.

Fondation à but non lucratif, Grassroots Economics cherche à « *donner aux communautés marginalisées les moyens de prendre en charge leurs propres moyens de subsistance et leur avenir économique* », notamment par la mise en œuvre de **programmes d'autonomisation économique**.

En 2018, Grassroots Economics a basculé d'un modèle de monnaie complémentaire « traditionnelle »[55], qui prenait la forme de coupon au format papier, circulant à côté de la monnaie nationale, le shilling kényan, à un modèle numérique et géré *via* un protocole blockchain assorti d'un token.

Ce projet de *Community Inclusion Currency* est *open source* et extrêmement bien documenté, que ce soit d'un point de vue technique[56] mais aussi opérationnel, notamment à travers des cours en ligne (*Massive open online course* - MOOC, formation en ligne ouverte à tous) pour apprendre à développer une monnaie communautaire papier avant de suivre une formation pour déployer une monnaie complémentaire basée sur leur blockchain.

De plus, Grassroots Economics est *blockchain agnostic*, et n'a pas hésité à changer de protocole pour chercher à optimiser au mieux l'architecture technique et l'utilisabilité du service.

En 2018, Grassroots Economics utilisait POA network[57], une *sidechain** de la blockchain publique Ethereum reposant sur la preuve d'autorité* (*Proof of Authority*) pour émettre les monnaies communautaires inclusives (CIC), ainsi que sur le protocole Bancor, à l'époque un exchange centralisé (CEX*) également développé sur Ethereum, permettant ainsi de rendre les différentes CIC convertibles entre elles.

En 2021, Grassroots s'est appuyée sur xDai chain, la blockchain publique de MakerDAO (voir *supra*) pour émettre les CIC, tandis qu'Uniswap a pris le relais de Bancor. Ces deux changements ont permis à Grassroots de reprendre la main sur son système de conversion des CIC tout en diminuant les frais de transactions. Depuis 2022, Grassroots développé sa propre blockchain, la Kitabu chain[58], créée à partir d'une copie de la blockchain publique permissionnée Bloxberg[59].

55 Avant que Grassroots Economics ne devienne entièrement numérique, ils ont construit des monnaies communautaires en utilisant des bons en papier de 2010 à 2018 au Kenya. Leur MOOC donne quelques explications sur comment et pourquoi ils ont fait cela : https://www.grassrootseconomics.org/pages/mooc.html
56 « Karibu to Grassroots Economics » Docs », Grassroots Economics, Grassroots Economics Website, retrieved May 10 ,2022, https://docs.grassecon.org/
57 POA Network: https://www.poa.network/
58 Kitabu chain: https://docs.grassecon.org/software/kitabu/
59 L'infrastructure bloxberg est une blockchain publique permissionnée établie par un consortium d'organismes de recherche afin de fournir aux scientifiques des services décentralisés partout dans le monde. Source : Bloxberg, https://bloxberg.org

La Kitabu chain présente les avantages de pouvoir opérer sans connexion internet, et surtout, de ne pas faire supporter de frais de transactions aux bénéficiaires des CIC.

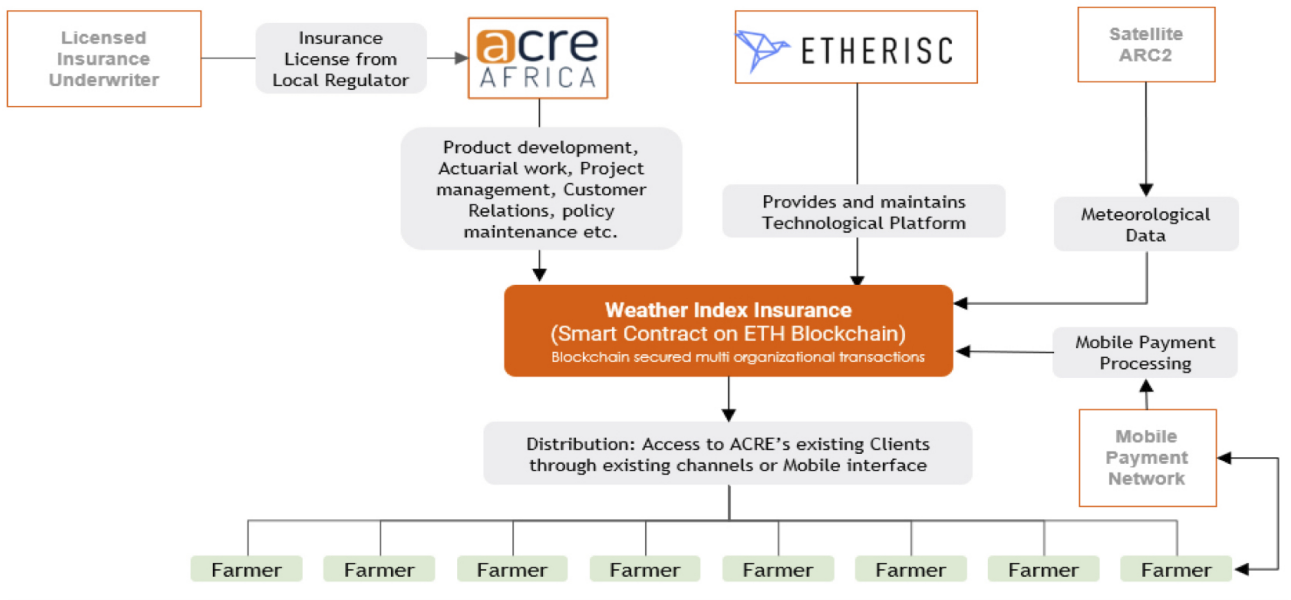
Une étude[60] publiée en janvier 2022 a été menée par Rebecca Mqamelo de l'université de Minerva aux Etats-Unis et porte sur l'analyse de l'usage de la monnaie d'inclusion communautaire de Grassroots Economics exécutée sur la blockchain xDAI de MakerDAO (voir paragraphe "DeFi - emprunter, épargner, investir"). L'étude présente les résultats de ce qui pourrait être le premier essai de contrôle randomisé au monde sur une monnaie communautaire. Des bénéficiaires situés à Nairobi, au Kenya, ont reçu l'équivalent de 30 dollars en crypto-actif local et complémentaire, ce qui a permis une analyse d'impact du programme de transfert d'argent. Les résultats, rendus publics, montrent que la circulation de la monnaie d'inclusion communautaire remplit son rôle de véhicule financier et a également mis en lumière « *les différences entre les effets du traitement pour les hommes et les femmes, ce qui suggère que les déséquilibres entre les sexes persistent* ». C'est en tout cas l'une des premières étude quantitative et qualitative dans le domaine des « Crypto for Good », qui montre que « *les monnaies d'inclusion communautaires sont un outil puissant permettant aux communautés de modifier la structure de leur économie locale de l'intérieur*[61] ».

Assurances

Le marché de l'assurance est concentré dans les mains de quelques grands groupes internationaux, parmi lesquels AIA Group Limited (Hong-kong), China Life Insurance (Chine), Prudential plc (Royaume-Uni). Ces géants de l'assurance ont commencé à s'intéresser aux blockchains à partir de 2018, principalement pour fluidifier les processus de paiement ou tenter de repérer les fraudes. Des projets blockchain dans le domaine de l'assurance ont émergé deux ans auparavant, notamment avec la création d'**Etherisc** en 2016 à Munich en Allemagne, par Christoph Mussenbrock, Stephan Karpischek et Renat Khasanshyn ou encore **Arbol**, créé à New York en 2018**.**

Etherisc développe un « *protocole pour les assurances décentralisées*[62] », pour notamment rendre « *l'achat et la vente d'assurance plus efficace qu'avec les assurances traditionnelles, mais également permettre une réduction des coûts opérationnels tout en offrant une meilleure transparence des opérations*[63] ». Basé sur la blockchain publique Ethereum, Etherisc développe un protocole, les *smart contracts** et une plateforme blockchain appelée « Generic Insurance Framework ». En fournissant cette infrastructure *open source* et en libre accès pour l'assurance décentralisée, quiconque souhaite créer ses propres produits d'assurance peut

60 « Community Currencies as Crisis Response: Results From a Randomized Control Trial in Kenya » www.frontiersin.org Rebecca Mqamelo* Minerva University, San Francisco, CA, United States, January 3, 2022. https://www.frontiersin.org/articles/10.3389/fbloc.2021.739751/full#h1
61 *Ibid.*
62 « Make Insurance Fair and Accessible », Ethersic, Ethersic website, retrieved May 10, 2022, etherisc.com/
63 *Ibid.*



System and relevant actors of the Etherisc Weather Index Insurance in Kenya
Source : Blockchain for Climate Action and the Governance Challenge Report from INATBA and CLI, https://climateledger.org/resources/Blockchain-for-Climate-Action-and-the-Governance-Challenge.pdf

utiliser la plateforme. Une trentaine d'applications ont déjà été testées, de l'assurance commerciale aux solutions dédiées au secteur non lucratif telles que les mutuelles, l'assurance de pair-à-pair, les modèles coopératifs ou encore de nouvelles structures d'assurances, comme celle lancée au Kenya en octobre 2020. Dans ce pays, l'offre d'assurance classique serait défaillante en raison « *d'une couverture insuffisante, de retards dans les paiements, du coût élevé des primes et d'un manque de transparence et de confiance*[64] ».

Etherisc, avec l'Agriculture and Climate Risk Enterprise Ltd (ACRE), un intermédiaire d'assurance agréé qui fournit des solutions de gestion des risques pour réduire les risques agricoles et climatiques au Kenya, ont mis en place une assurance décentralisée à destination des agriculteurs locaux, entièrement automatisée et indexée sur les conditions météorologiques, avec le support de Chainlink et de la Fondation Ethereum. Lancée en novembre 2020, elle comptait un an plus tard « *12 567 agriculteurs assurés avec au moins 511 petits agriculteurs en mesure de recevoir un paiement de mi-saison pendant la longue saison des pluies 2021*[65] ».

Le processus est le suivant : un agriculteur paye des semences dont le prix inclut une prime d'assurance paramétrique, c'est à dire une assurance corrélée aux conditions

64 « Reunion with our Partners In Nairobi: A recap of Etherisc's week in Kenya », Etherisc, https://blog.etherisc.com/reunion-with-our-partners-in-nairobi-a-recap-of-etheriscs-week-in-kenya-a0560ffea77f
65 « Reimagining agriculture insurance using blockchain technology », Jean Eyase, Acreafrica.com, November, 11, 2021, https://acreafrica.com/reimagining-agriculture-insurance-using-blockchain-technology/

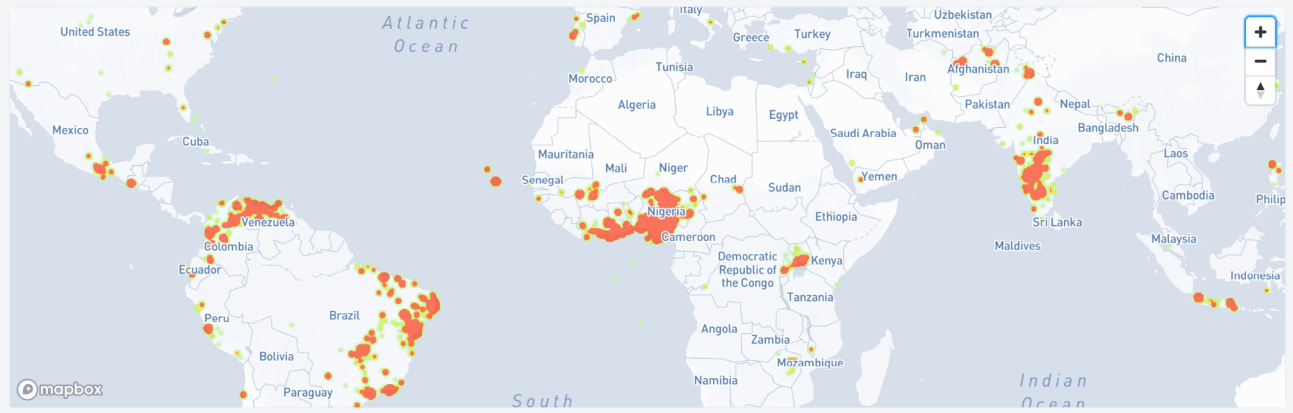


Tableau de bord global Impact Market
Source : https://impactmarket.com/fr-FR/global-dashboard

météorologiques ; l'agriculteur qui plante ses semences utilise un identifiant généré par SMS avec un simple *feature phone** afin de fournir des informations à la fois personnelles et agricoles. Une fois que le contrat d'assurance décentralisé est lancé, le programme interagit de manière autonome suivant les données correspondant à l'assurance de l'agriculteur.

L'ACRE propose quatre assurances[66] : **(1)** *Une couverture indexée sur la météo*, basée sur des données pluviométriques recueillies par satellite. La couverture est déclenchée lorsque les précipitations sont inférieures à certains seuils déterminés selon les besoins de la culture **(2)** *Une couverture de l'indice d'humidité du sol*, basée sur des données d'humidité du sol collectées également par satellite. La couverture se déclenche lorsque l'humidité du sol est inférieure à certains seuils déterminés selon les besoins de la culture *(3) un index de végétation,* basé sur la couverture végétale, adapté pour les zones arides et semi-arides. La couverture est déclenchée lorsque la quantité de végétation est inférieure à la quantité suffisante pour permettre la vie animale. Et enfin **(4)** *une couverture des cultures multi péril* qui couvre l'agriculteur en cas de sécheresse, de précipitations excessives, d'inondations, de grêle, de tempêtes de vent, de gel ou encore de feu, la liste n'étant pas exhaustive.

De plus, plutôt que de s'appuyer sur un tiers de confiance, centralisé, pour obtenir les données météorologiques, le *smart contract* est connecté à des « réseaux d'oracle* décentralisé » *Decentralized Oracle Networks*, c'est à dire proposé par un panel d'intermédiaires qui fournissent des informations externes et vérifiées *via* une autre blockchain ou tout autre service. L'oracle utilisé par Etherisc pour ce programme est **Chainlink**, un *Decentralized Oracle Networks* créé en 2017 à New York, aux Etats-Unis, par Sergey Nazarov et Steve Ellis.

66 « Who we are », ACRE Africa, ACRE Africa website, retrieved May 10, 2022, https://acreafrica.com/

En décembre 2021[67], plus d'un millier de projets blockchain s'appuient sur le réseau d'oracle décentralisé créé par Chainlink au sein duquel 77 milliards de dollars de crypto-actifs sont sécurisés sur le réseau, dans des *smart contracts**. Le réseau **Chainlink** est maintenu par quelque 700 nœuds qui mettent en œuvre des *smart contracts* hybrides, c'est à dire reposant sur des composants qui s'exécutent à la fois *on-chain**, sur une blockchain, n'importe laquelle, et des composants qui s'exécutent *off-chain** sur leur réseau d'oracle décentralisé, et qui garantit l'intégrité, la véracité et la confidentialité des données.

Chainlink est ainsi intégré aux *smart contracts** d'Etherisc pour fournir des données météorologiques en temps réel. Lorsque survient une intempérie couverte par le *smart contract**, ce dernier déclenche automatiquement le paiement de l'indemnisation. Cette solution permettrait, selon l'INATBA[68], « *de réduire les primes jusqu'à 30 % et de ramener le cycle des sinistres de trois mois à une semaine (...) et les paiements sont effectués via M-PESA, directement sur le téléphone portable de l'agriculteur*[69] ». Tous les paiements sont enregistrés sur la blockchain d'Etherisc pour fournir une transparence des transactions. Etherisc a annoncé que 6 000 agriculteurs[70] allaient être indemnisés avant la fin de la saison 2021, *via* le système de paiement mobile M-Pesa pour leurs récoltes perdues ou affectées. L'ACRE et Etherisc ont pour ambition d'assurer, dans les prochaines années, 250 000 agriculteurs[71] en Afrique de l'Ouest.

Revenu universel

Selon la définition du Mouvement français pour un Revenu de Base (MFRB), « *le revenu de base, appelé aussi revenu d'existence, revenu inconditionnel ou encore allocation universelle, est un revenu versé par une communauté politique à tous ses membres, sur une base individuelle, sans conditions de ressources ni obligation de travail*[72] ». Pour quel montant ? A qui ? Combien de temps ? Qui finance ? Quel impact sur la société et le travail ? Les innombrables questions liées à la mise en place d'un revenu universel sont posées depuis le 17e siècle, notamment par Locke et la « clause lockéenne », qui justifiait une allocation universelle comme la contrepartie à la propriété privée de la terre au profit de ceux qui n'en bénéficiaient pas. Ces questions restent contemporaines et sont portées par des philosophes, des penseurs

67 « Chainking data feeds », Chainlink, Chainlink website, retrieved May 10, 2022, data.chain.link/
68 International Association for Trusted Blockchain Applications: https://inatba.org
69 « Climate Action and Governance with Climate Ledger Initiative », INATBA, June 1, 2021, https://inatba.org/reports/climate-action-governance-challenge/
70 Etherisc onboards 17K Kenyan farmers covered by blockchain-based crop insurance, Turner Wright, cointelegraph.com Jul 21, 2021, https://cointelegraph.com/news/etherisc-onboards-17k-kenyan-farmers-covered-by-blockchain-based-crop-insurance
71 *Ibid*.
72 « Revenu de Base », Novethic, consulté le 10 mai 2022, https://www.novethic.fr/lexique/detail/revenu-de-base.html

mais aussi des institutions, des syndicats, des Organisations internationales, des associations, indépendamment de la couleur politique de chacun.

Plusieurs initiatives blockchain cherchent ainsi à mettre en œuvre des formes de revenu universel ou revenu de base, parmi lesquelles **Circles** (2015) portée par la Trustlines Foundation, **GoodDollar** (2017), **Baza Foundation** (2018), **Idena** (2019) ou encore **ImpactMarket** (2020), dans des formes différentes. Par exemple, Baza Foundation se présente comme « *une plateforme numérique construite avec l'objectif de réimaginer une organisation à but non lucratif en adaptant les principes du revenu de base, des contrats intelligents et de la technologie du ledger* sécurisé[73] *»*. Circles, porté par Trustlines Network[74] explique être « *une monnaie alternative qui permet à des groupes organisés de personnes de s'assurer mutuellement un revenu de base, plutôt que de dépendre de l'État*[75] ».

Impact Market, quant à lui, se définit comme « *un protocole décentralisé de lutte contre la pauvreté qui permet la création et la distribution d'un revenu de base inconditionnel entre les communautés et leurs bénéficiaires, en fonction de leurs besoins* ». Impact Market se présente comme un protocole décentralisé de réduction de la pauvreté. C'est une Organisation autonome décentralisée (DAO*) utilisant un token appelé $PACT. Le protocole utilise le cUSD de Celo (voir *supra*) comme principale monnaie numérique, tout en fonctionnant de manière automatique par le biais de *smart contracts**.

Depuis la mise en place d'Impact Market, 236 communautés réparties dans 44 pays dans le monde, parmi lesquels le Brésil, le Venezuela, le Kenya, le Ghana, l'Inde, le Nigéria, le Cap Vert reçoivent une forme de revenus mensuels financés par des dons et gérés localement par « *des dirigeants communautaires et des organisations sociales, gouvernementales ou locales, qui définissent les paramètres initiaux et ajoutent/suppriment les bénéficiaires*[76] ». Chaque communauté reçoit une allocation quotidienne par bénéficiaire, entre l'équivalent de 0,5 centimes de dollar à 1,5 dollars. Le Brésil, le Nigéria et le Vénézuéla comptent le nombre le plus important de bénéficiaires. En mai 2022, 5 233 donateurs ont versé 2 632 313 cUDS (Celo) répartis entre 43,810 bénéficiaires qui perçoivent en moyenne 0,55 $ par jour pendant, en moyenne, 40 mois.

Impact Market fait interagir trois communautés au sein d'une Organisation autonome décentralisée* : **(1)** Des « gestionnaires de communauté », en charge de soumettre une communauté

73 « Baza Coin », Baza Foundation, Baza Foundation website, retrieved May 10 2022, https://baza.foundation/
74 « About Trustlines », Trustlines, Trustlines website, retrieved May 10 2022, https://trustlines.network/
75 « A basic income system for communities », Join Circles, Join Circles website, retrieved May 10, 2022, https://joincircles.net/
76 « Tableau de bord Impact Market », Impact Market, consulté le 10 mai 2022, https://www.impactmarket.com/fr-FR/global-dashboard

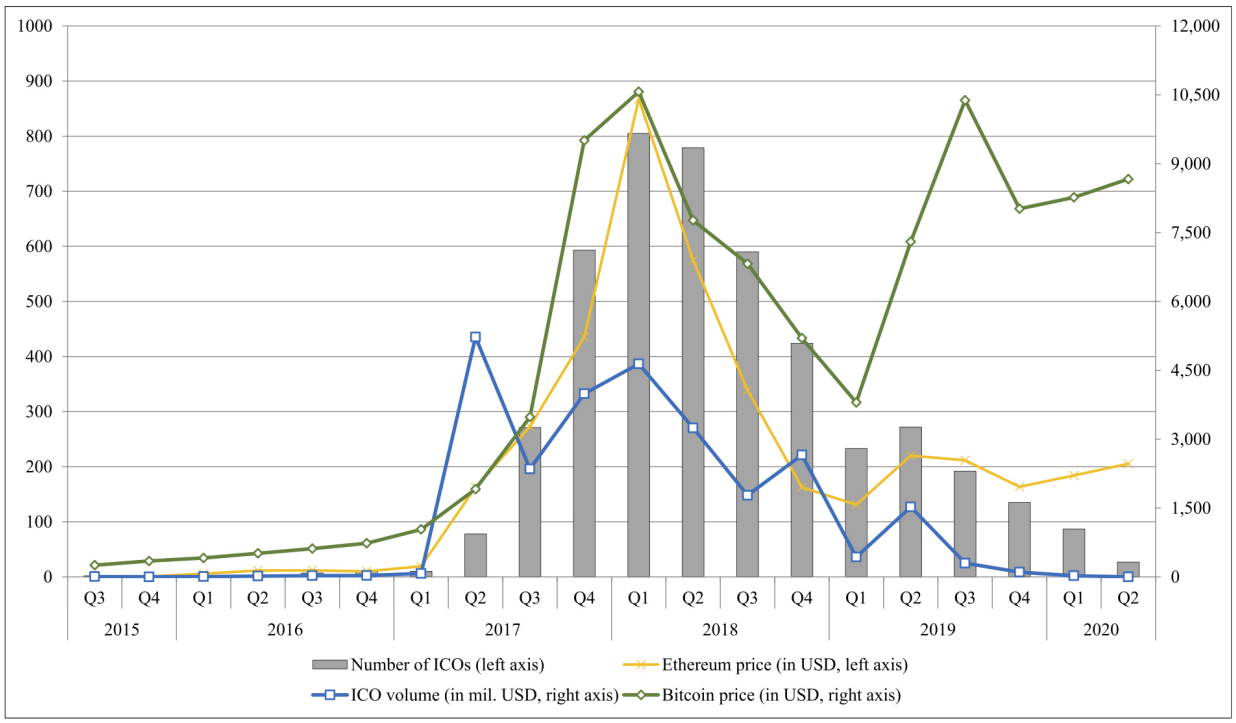
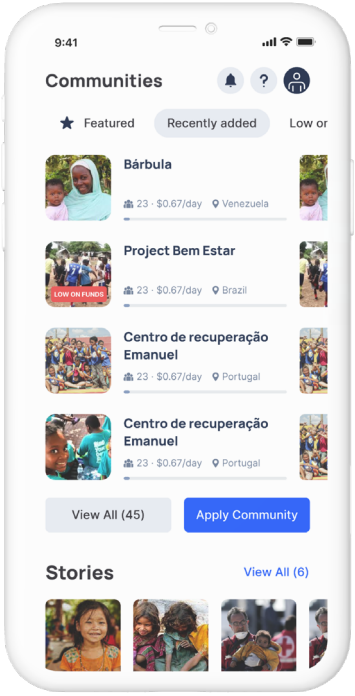


Fig. 1. Evolution of the number of ICOs, ICO volume, and Bitcoin price.
Source : Bellavitis, C., Fisch, C., & Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation. Journal of Business Venturing Insights 15 (2021). doi:10.1016/j.jbvi.2020.e00213

pour approbation puis d'en gérer les bénéficiaires. Ce sont en général des institutions sociales locales qui ont un accès direct aux bénéficiaires finaux et s'adressent autant que possible à ceux qui en ont le plus besoin rapidement. Un gestionnaire de communauté postule en ligne, en fournissant un certain nombre d'informations ainsi que les détails d'un contrat de revenu de base pour les bénéficiaires. Une fois accepté comme gestionnaire de communauté, la ou les personnes pourront ajouter des bénéficiaires qui pourront alors réclamer une aide correspondant aux fonds à disposition. Deux applications mobiles, interconnectées, sont nécessaires, l'application Valora, un portefeuille mobile de crypto-actifs compatibles avec les DApps* construites sur la blockchain Celo, et l'application impactMarket, permettant de gérer la communauté. **(2)** Des bénéficiaires, les personnes qui auront accès à un revenu de base. Ils devront être équipés d'un *smartphone* et télécharger les deux applications Valora et ImpactMarket. **(3)** Les donateurs, ceux qui font un don pour soutenir le projet. Lorsque les donateurs font un don à l'Organisation autonome décentralisée (DAO*) en cUSD, ils deviennent éligibles à recevoir des tokens $PACT comme récompense. Les donateurs peuvent également choisir d'aider spécifiquement une communauté, visible sur l'application Valora[77].

77 « If you can text, you can crypto », Valora, Valora website, retrieved May 10, 2022, https://valoraapp.com/fr

Outre le cUSD, les donateurs peuvent effectuer un don en monnaie fiat, en Bitcoin, en Ether ou encore *via* Paypal en utilisant eSolidar, mais ils ne recevront pas de token $PACT en récompense. Une quatrième communauté peut également participer à l'écosystème, les marchands locaux, qui peuvent accepter les cUSD, afin que les bénéficiaires se fournissent en nourriture, en électricité, en eau et autres produits ou services de la vie courante. Impact Market utilise le Celo Dollar, (cUSD), un crypto-actif stable* indexé sur le dollar américain déployé par Celo dont les frais de transactions sont généralement autour de 0,001 USD par transaction.



Impact Market community
Source : Impact Market, retrieved May 10 2022, https://docs.impactmarket.com/communities/how-to-apply-a-community

L'écosystème est décentralisé parce que les donateurs choisissent vers qui s'adressent leurs fonds, et que ce sont des *smart contracts** qui se chargent de les répartir selon les termes du contrat de revenu universel de la communauté visée. Au niveau local, les gestionnaires de communautés ne manipulent pas de fonds mais ouvrent et ferment les comptes de bénéficiaires qui reçoivent directement l'aide dans leur portefeuille de crypto-actif. Le protocole d'ImpactMarket, *open source*[78], est régi par les détenteurs de jetons $PACT qui votent sur des propositions. La DAO* est constituée de trois *smart contracts**, à travers lesquels tout ce qui se passe sur le protocole passe par le vote de « propositions » qui concernent toutes les décisions prises par la communauté, comme, par exemple, la mise à jour d'un contrat pour l'allocation de fonds provenant de la trésorerie, la création ou la fermeture de communautés etc.

Il est également possible pour une organisation humanitaire ou une organisation internationale d'utiliser ImpactMarket en finançant le fonds du montant de l'aide apportée, afin de gérer sur le terrain les bénéficiaires du programme.

78 Impact Market Github: https://github.com/impactMarket/impact-market-smart-contracts

Good Dollar
ou le « Staking for Good »[79]

Good Dollar est une ONG créée par Yoni Assia, CEO d'eToro, une société de trading multidevises fondée en 2007 en Israël. Après avoir publié, en novembre 2008, un essai intitulé « Good Dollar – The Visible Hand »[80] présentant le concept, c'est en 2018 que le projet est lancé. Good Dollar est un outil en ligne pour distribuer un revenu de base universel dans un crypto-actif appelé G$, qui s'appuie sur les protocoles de la Finance décentralisée (DeFi) de la blockchain Ethereum et sur la *sidechain** Fuse.io. Le code informatique, *open source*, réunit trois communautés : (1) Les financeurs : Plutôt que d'abonder directement aux fonds Good Dollar, les financeurs déposent des DAI (MakerDAO) ou Ether (Ethereum) dans des protocoles de staking* ou des mécanismes tiers *via* le GoodDollar Trust et, plutôt que percevoir les intérêts de cette immobilisation, ces derniers sont versés dans la trésorerie de Good Dollar. (2) Les bénéficiaires de l'UBI : Le caractère universel de Good Dollar n'impose comme condition pour recevoir des token Good Dollar que celle de s'inscrire, télécharger un portefeuille* (*wallet*) et réclamer (*claim*) de manière quotidienne les Good Dollar générés par les opérations de staking* des financeurs.

Chaque jour les Good Dollar sont répartis entre tous les bénéficaires les ayant réclamés.

En mai 2022, 2,4 millions de Good Dollar étaient distribués quotidiennement, soit l'équivalent de 454 US $. (3) Enfin, les marchands sont les commerçants qui acceptent d'être payés en Good Dollar, qui peuvent être convertis dans d'autres crypto-actifs parmi lesquels l'Ether ou le DAI. Selon les données présentées[81] par Good Dollar, 542 millions de G$ ont été versés à 427 549 personnes depuis la création du projet, soit l'équivalent de 90 651 $. En mai 2022, 1 G $ = 0,00018 $. En avril 2021, les pays où la demande de G$ a été la plus forte sont le Nigéria, le Vietnam, le Brésil, l'Inde et l'Indonésie.

Financement participatif

Le financement participatif, à ne pas confondre avec une *initial coin offering* (ICO*), est une opération qui consiste en la levée de fonds *via* l'émission d'actifs numériques échangeables contre des crypto actifs, lors de la phase de démarrage du projet. L'intérêt de ce processus de levée de fonds est d'être accessible à quiconque possède des crypto-actifs, sans qu'un établissement financier ou un régulateur n'intervienne.

Des projets blockchains renouvellent le caractère centralisé des plateformes de financement participatif traditionnelles, parmi lesquels **eSolidar, ImpactMarket, Suretly, Topl, IcrowdU** ou encore **Raise** ou **WeiFund**.

79 « The GoodDollar Basic Income Economy », Gooddollar.org, retrieved May 17, 2022, https://whitepaper.gooddollar.org/the-gooddollar-basic-income-economy#staking-for-good
80 « Good Dollar – The Visible Hand », Yoni Assia, November 28, 2008, retrieved May 17, 2022, https://yoniassia.com/good-dollar-the-visible-hand/
81 Good dollar Dashboard, retrieved May 17, 2022, https://dashboard.gooddollar.org/

Par exemple, la *startup* **Raise** créée à Nairobi au Kenya en 2017 développe, selon son fondateur Marvin Coleby, une plateforme qui « *prépare les startups à lever des fonds grâce à un tableau de capitalisation automatisé, des certificats d'actions électroniques et une évaluation de l'entreprise et de la technologie* ». Parmi les différents services que proposent la plateforme figurent notamment la possibilité pour les actionnaires de consulter facilement et de manière sécurisée les données liées à leurs investissements. Les bénéficiaires des fonds peuvent également émettre des actions numériques (*digital share*) et des certificats convertibles (*convertible certificates*) afin de réduire les procédures administratives et les coûts opérationnels des levées de fonds traditionnelles[82]. Raise propose une plateforme qui automatise les aspects financiers et réglementaires des levées de fonds aidant les *startups* de l'écosystème africain.

Autre projet, **WeiFund**, créé à Toronto en 2015. C'est une plateforme de *crowdfunding* à but non lucratif, décentralisée et *open source*, construite sur Ethereum. WeiFund permet de transformer les contributions en actifs numériques garantis par contrat, tels que des actions ou des jetons, qui peuvent être utilisés, échangés ou vendus dans l'écosystème Ethereum.

Co-financé par l'Union européenne à travers le programme Smart Growth et par le Centre national de recherche et de développement de Pologne, **Tecra** développe depuis 2018 une plateforme décentralisée de *crowdfunding*, **Tecra Space**, soutenue par une crypto-devise, le **TecraCoin (TCR)**, actuellement échangeable sur la bourse d'échange centralisée Hotbit et la bourse d'échange décentralisée Uniswap (DEX*), avant que soit développé leur propre bourse d'échanges décentralisée, **Tecra DEX**[83].

Selon l'entreprise, Tecra « *offre aux scientifiques et aux innovateurs un moyen facile de lever des fonds grâce au* crowdfunding*, de bénéficier de la sécurité des brevets et de frais réduits, ainsi que de remboursements rapides après la réalisation des bénéfices du projet*[84] ».

Chaque projet lancé *via* la plateforme de *crowdfunding* sera assorti de son propre token, qui pourra être acheté avec des Ether, le crypto-actif stable* Tether, des TecraCoin, mais également par carte de crédit, PayPal ou virement bancaire. L'investissement minimum est deun TCR, soit entre 50 centimes (cours au 1er janvier 2021) et deux dollars (cours au 7 juillet 2021). D'un point de vue technique, le TecraCoin est un jeton ERC-20 enregistré sur une blockchain publique avec permission basée sur Ethereum[85].

82 « How Raise works to help prepare your startup for investment », Marvin Coleby (CEO), Intercom website, retrieved 10 May, 2022, https://intercom.help/raise/en/articles/3665904-what-is-raise
83 « Crypto crowdfunding platform launches DEX for project-specific tokens », Connor Sephton, Cointelegraph website, May 24, 2021, https://cointelegraph.com/news/crypto-crowdfunding-platform-launches-dex-for-project-specific-tokens
84 Tecra: https://tecra.space/
85 « Tecra Space Warsaw », Krzysztof Bochenek, PO Poland, January 20, 2021, https://www.24-7pressrelease.

Le TecraCoin un crypto-actif déflationniste dont le nombre de jetons pré-minés sera progressivement réduit (*burnt* - brûlé) par les nœuds de validation. Tecra a remporté le Startup Grand Slam au World Blockchain Summit de Taipei en 2019, et a également été finaliste de la Singularity University pour le prix des dix meilleures *startups* d'Europe de l'Est, décerné sur le Campus Google à Varsovie.

En décembre 2021, douze ans après sa création Kickstarter a annoncé vouloir basculer leur plateforme de financement participatif centralisée vers un nouveau modèle, cette fois-ci décentralisé, et qui s'appuiera sur la blockchain Celo (voir *supra*). Selon son fondateur Perry Chen, « *dans les années à venir, nous pensons que de larges pans de l'internet seront entièrement reconstruits par des réseaux ouverts et décentralisés de contributeurs, qui participent à la conception, au fonctionnement, à la gouvernance et même à la propriété de la technologie elle-même*[86] ».

Finance inclusive

Si la finance inclusive existe, c'est bien que la finance, dans sa forme classique, exclut. Celle traditionnelle, reposant sur les banques et les institutions financières. La finance, dite inclusive, naît entre les années 1970 et 1980 avec le microcrédit moderne développé par l'économiste bengladais Muhammad Yunus, qui recevra le prix Nobel de la paix en 2006. Elle se développe depuis en tentant d'adapter les réglementations du système financier traditionnel à la microfinance, au financement participatif, à la banque sur téléphone portable etc. à destination des personnes les plus défavorisées, exclues du système bancaire.

Hiveonline lancé en 2016 à partir du Danemark, **Waba**, créé en Argentine depuis 2017 ou encore **Ethic Hub**, créé en 2019 en Espagne sont quelques-unes de ces initiatives. Par exemple, **Ethic Hub**, créé en 2019 en Espagne, est une entreprise sociale qui met en relation des investisseurs avec de petits agriculteurs afin qu'ils puissent mener à bien leurs récoltes, notamment de café, et les vendre sur des marchés sans intermédiaire pour que 50% des profits leur reviennent directement[87]. EthicHub s'adresse particulièrement aux agriculteurs non bancarisés habitant le Mexique. L'équipe a développé une plateforme pair-à-pair de financement (*crowdlending*) où de nombreux petits investisseurs, 20 euros minimum, financent les activités agricoles de petites communautés agricoles tout en recevant des intérêts sur les prêts.

En 2020, EthicHub a décidé[88] de migrer ses opérations de la blockchain **Ethereum** vers **xDai Chain**, une *sidechain** ou Layer 2 basée sur Ethereum qui utilise un mécanisme de consensus basé sur la

com/press-release/478789/europe-is-gearing-up-for-the-blockchain-revolution-altcoins-on-the-rise
86 « The Future of Crowdfunding Creative Projects », Perry Chen & Aziz Hasan, Kickcstarter website, December 9, 2021, https://www.kickstarter.com/articles/the-future-of-crowdfunding-creative-projects
87 « Specialty Coffee » EthicHub, retrieved May 10, 2022, https://shop.ethichub.com/en
88 « Why did we start using xDai in EthicHub ? », Equipo EthicHub, EthicHub website, retrieved May 10, 2022, https://help.ethichub.com/hc/en-us/articles/360013429458-Why-did-we-start-using-xDai-in-EthicHub-

preuve de participation* (Proof-of-Stake). Lancé depuis fin 2018, xDai Chain utilise le crypto-actif stable*, xDai, comme crypto-devise native. EthicHub résout ainsi plusieurs problèmes dont notamment celui de la rapidité d'exécution et surtout le coût des transactions. Depuis son lancement en 2019, EthicHub a reçu plus de 7 000 micro investissements, distribués à 240 agriculteurs répartis dans 17 communautés, impactant indirectement près d'un millier de familles[89].

Hiveonline se décrit comme une entreprise donnant accès au crédit et aux marchés à de petits exploitants exclus financièrement et à leurs écosystèmes locaux. L'une des plateformes de Hiveonline repose sur « *une blockchain permettant de distribuer des bons (vouchers) de manière sécurisée et une crypto-devise stable* afin de fournir de l'argent numérique en monnaie locale avec des enregistrements sûrs et immuables* ». L'entreprise aime à dire faire de « la finance numérique durable sans téléphone ». (Voir projet exemplaire en fin de chapitre).

Investissement d'impact

L'investissement à impact social est défini comme « *un investissement qui allie explicitement retour social et retour financier sur investissement*[90] ». Il s'agit de proposer à des investisseurs, qu'ils soient particuliers ou entreprises, de financer des projets aux impacts sociaux ou environnementaux positifs. Parce que l'usage d'une blockchain permet de se passer des intermédiaires entre un investisseur et son bénéficiaire, de nombreuses initiatives reposant sur une blockchain ont émergé, dont notamment la plateforme **Sun Exchange**.

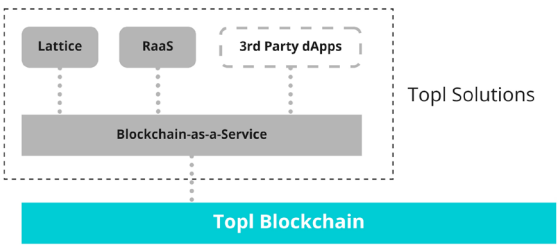
Fondée en Afrique du Sud en novembre 2015 par Abe Cambridge, la plateforme **Sun Exchange**, (dont nous parlons également dans le chapitre « Energie »), souhaite démocratiser le **financement des énergies renouvelables par le *crowdfunding***. C'est une place de marché de micro-bail qui met en relation des investisseurs, particuliers et entreprises, avec les bénéficiaires d'installations solaires dans les zones rurales d'Afrique du Sud, avec la promesse d'un rendement de 10 % sur un contrat de 20 ans. La plateforme utilise la blockchain Bitcoin pour les paiements transfrontaliers afin qu'il n'y ait aucun intermédiaire entre les bénéficiaires de l'installation, qui paient leur électricité, et les investisseurs qui ont participé à l'achat des panneaux solaires. Suite à une première campagne de financement participatif entre janvier et novembre 2015, l'entreprise a construit une première centrale solaire dans une école de la région du Cap. Trois ans plus tard, la plateforme comptait 6 000 investisseurs enregistrés et a construit sept centrales solaires. En 2022, plus de 40 centrales solaires, pour une capacité électrique totale de 5,2 GWh d'énergie propre ont été créées, grâce à l'investissement de particuliers et d'entreprises répartis dans 180 pays dans le monde. Les bénéficiaires

89 « Inversión de Impacto Protegida », EthicHub, retrieved May 10, 2022, https://www.ethichub.com/
90 Comité français sur l'investissement à impact social.

des installations photovoltaïques sont principalement des écoles, des maisons de retraite, des petites et moyennes entreprises, des parcs naturels et des associations à but non lucratif qui, dorénavant, paient leur électricité 20 à 30 % moins cher. Les économies réalisées servent notamment à fournir une éducation de qualité aux enfants, des environnements de vie positifs aux résidents âgés et des soins aux animaux sauvages vulnérables.

Verification d'impact

Topl, Ixo Foundation ou encore Proof of Impact sont quelques-unes de ces initiatives ayant pour objectif de « tokeniser » l'impact de l'activité des organisations. **Topl**, créé à Houston aux Etats-Unis en 2017 se présente comme « *entreprise technologique ESG qui construit une blockchain pour aider les entreprises à prouver les pratiques éthiques et durables* ». C'est tout un écosystème que souhaite développer l'entreprise, notamment à travers deux tokens, un premier de gouvernance ainsi qu'un crypto-actif stable*, et dont toutes les briques seront développées d'ici à la fin de l'année 2022.



Topl projette de lancer une blockchain publique, *open source*, dont le mécanisme de consensus sera basé sur la preuve d'enjeu*.

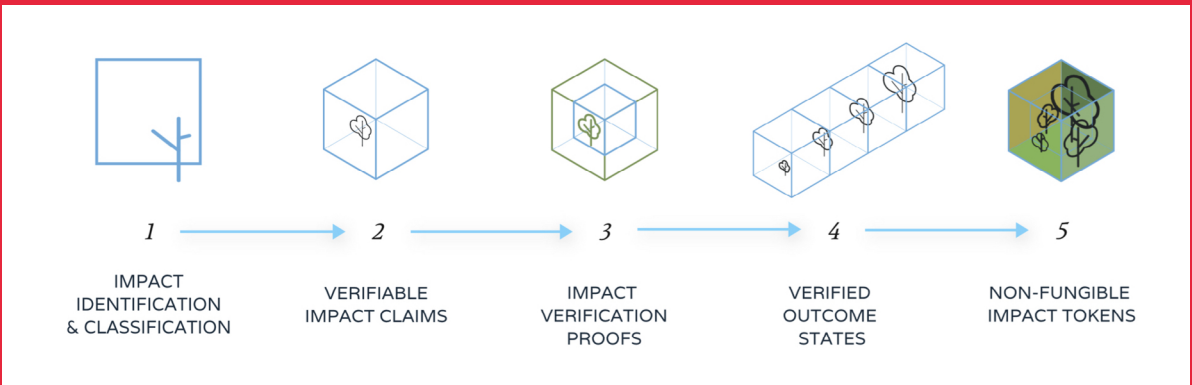
Ixo Foundation a aussi été créé en 2017, à Zug en Suisse. La Fondation IXO développe le protocole du même nom sur la blockchain publique **Cosmos**. L'objectif du protocole IXO est d'enregistrer des « faits vérifiables » dans une blockchain publique, notamment des données liées à l'environnement, l'économie et les impacts climatiques. Il s'agit d'adjoindre à la finance décentralisée des mécanismes de durabilité, *Sustainable DeFi*, déterminés par des changements d'état extrinsèques du monde réel : un certificat d'énergie renouvelable, un certificat de crédit carbone et d'autres « faits vérifiables », notamment grâce au fait que « *les changements d'états du monde réel peuvent désormais être contrôlés, vérifiés et attribués de manière fiable à des agents, entités, événements et investissements identifiés*[91] » explique le site web d'Ixo Foundation.

IXO est construit sur la blockchain publique Cosmos, dont l'ambition est de devenir « l'internet des blockchains » en offrant une interopérabilité sécurisée entre les services de différentes blockchains publiques. En s'appuyant sur l'écosystème propre à la blockchain Cosmos, IXO peut interagir avec n'importe quelle autre blockchain sur Cosmos mais également utiliser des ponts vers les autres écosystèmes dont notamment les blockchains publiques Ethereum, Cardano ou encore Polkadot. L'activité d'IXO a débuté en 2015, tout d'abord au sein du TrustLab basé en Afrique du Sud, financé par les fonds

91 Ixo Foundation: https://www.ixo.world/protocols

La tokenisation d'impact selon IXO Foundation

Source : https://www.ixo.world/protocols - Traduction : Blockchain for Good



1. Identification de l'impact
Les observations sur l'état du monde sont identifiées à l'aide d'identifiants décentralisés (DID)* et classées en fonction du contexte sémantique à l'aide de schémas de données liées.

2. Réclamations d'impact
Des déclarations d'impact vérifiables sont émises et signées cryptographiquement par des agents identifiés et authentifiés. L'utilisation d'applications clientes, telles que le portefeuille d'impact mobile ixo, permet de capturer les données de réclamation au niveau de la mise en œuvre des processus du monde réel qui créent et observent le changement.

3. Vérification de l'impact
Les déclarations d'impact, avec leurs données certifiées comme preuve, sont évaluées par des agents vérificateurs indépendants et certifiés.
Les vérificateurs utilisent des rubriques d'évaluation et des méthodes statistiques standardisées pour déterminer si chaque déclaration peut être approuvée. Ils délivrent des preuves de vérification qui attestent que les déclarations remplissent les conditions requises pour être approuvées.

4. Crédibilité de l'impact
Les collections d'allégations vérifiables au fil du temps, ainsi que leurs preuves de vérification et des informations supplémentaires - telles que les références vérifiables d'un exécutant de projet, sont combinées pour émettre une accréditation vérifiable pour un état d'incidences. Ce qui inclut un graphe des déclarations, des preuves et des références.

5. Tokenisation d'impact
Les jetons d'impact sont frappés avec des graphes d'actifs de données en tant que ressources liées, qui peuvent être récupérées par des utilisateurs autorisés à partir de points de service spécifiés - tels que les magasins de données confidentielles ixo Cellnode, d'une manière autorisée, en utilisant des capacités d'autorisation (zCaps). Les jetons d'impact non fongibles peuvent être configurés dans des mécanismes de financement basés sur les résultats, tels que les Alphabonds, échangés en tant qu'actifs numériques, ou utilisés pour créer de nouveaux types de régimes de propriété et de mécanismes de participation centrés sur les parties prenantes.

d'innovation de l'UNICEF, ainsi qu'un autre fond d'impact, appelé Innovation Edge[92] pour développer un premier projet, Amply.

Amply[93], mené avec l'UNICEF et le gouvernement d'Afrique du Sud a consisté à numériser la gestion d'un programme d'éducation d'Afrique du Sud en enregistrant sur la blockchain Ethereum la fréquentation à l'école maternelle d'enfants défavorisés et en émettant des tokens comme preuve d'impact en échange de subventions gouvernementales. En effet, le gouvernement sud-africain avait mis en place un programme de subvention de 200 millions de dollars à destination de 800 000 enfants défavorisés. Or pour accéder à ces aides, les enseignants devaient faire état de la présence ou non de chacun, à l'aide de cahiers au format papier, puis les présenter tous les trimestres à des administrateurs du ministère du développement social qui s'occupaient ensuite de débloquer les subventions école par école.

Avec Amply, chaque enfant s'est vu attribuer une identité numérique décentralisée afin que les enseignants enregistrent leur présence en générant une attestation vérifiable* (Voir Chapitre Identité et Propriété). Les attestations vérifiables ainsi que des métadonnées associées (lieu, date, heure de la collecte) étaient ensuite vérifiées par les administrateurs du ministère du développement social, générant, par le biais d'un *smart contract**, un token d'impact dont l'école se servait ensuite pour obtenir la subvention prévue par le gouvernement.

Selon l'International Institute for Sustainable Development, « *des applications comme Amply peuvent réduire la fraude et les coûts associés à ces programmes tout en donnant aux prestataires de services et aux bailleurs de fonds un aperçu précieux et la preuve que leur argent est bien dépensé. Les données sont accessibles sur la blockchain par n'importe qui, et elles permettent aux gouvernements, aux chercheurs, aux donateurs et aux ONG de prendre des décisions plus éclairées sur leur travail afin d'en optimiser l'impact* »[94].

Ce projet pilote s'est ensuite transformé en un contrat plus important en Inde, pour réitérer l'expérience à travers le « Quality Education India DIB », lancé en 2018 à l'Assemblée générale des Nations Unies à New York avec le gouvernement indien à Delhi.

Protéiforme et même complexe à appréhender, la plateforme IXO propose « *une norme ouverte pour produire des déclarations vérifiables* sur les changements de l'état du monde*[95] ». Chaque token d'impact représente un « état de résultat

92 Innovation Edge, retrieved May 17, 2022, https://innovationedge.org.za/
93 « Impact Tokens: A blockchain-based solution for impact investing », David Uzsoki, Patrick Guerda, International Institute for Sustainable Development | IISD.org, https://www.iisd.org/system/files/publications/impact-tokens.pdf
94 « Impact Tokens: A blockchain-based solution for impact investing », David Uzsoki, Patrick Guerda, International Institute for Sustainable Development | IISD.org, https://www.iisd.org/system/files/publications/impact-tokens.pdf
95 IXO Foundation White Paper, retrieved May 20, 2022, https://www.ixo.world/white-paper

vérifié », sous la forme d'un jeton non fongible* (NFT), qui est soutenu par des actifs de données d'impact et des preuves de vérification, avec des droits exécutables intégrés.

Pour la Fondation, les jetons d'impact seront amenés à remplacer tous les instruments négociables comme « *les certificats de réduction d'émissions vérifiés pour les crédits carbone, les certificats d'énergie renouvelable pour les énergies propres, les certificats de qualification pour les résultats éducatifs, les certificats de biodiversité pour les résultats en matière de nature, les certificats de vaccination pour les résultats en matière de santé ou tout autre état de résultat vérifié auquel les gens tiennent, pour lequel ils sont prêts à investir, à travailler ou à dépenser leur argent*[96] ».

Les données permettant de prouver « l'évolution d'un état » dans le monde réel proviennent de sources variées, parmi lesquelles des capteurs de l'Internet des objets (IoT), les enquêtes d'un utilisateur authentifié, de l'imagerie satellitaire ou les données collectées à partir des appareils connectés des participants à un projet. Les données doivent remplir des «preuves d'impact» prédéterminées afin que les prestataires de services puissent prétendre avoir réussi et que les investisseurs puissent recevoir leurs retours financiers.

En plus d'utiliser ces données pour vérifier l'état final d'un projet, ces données alimentent en continu un marché de prédiction interne entre les parties prenantes du projet, qui ajuste dynamiquement les paramètres, tels que les paiements d'intérêts liés à la possession du jeton d'impact. Appelé alphabond, ce mécanisme vise à accroître la sophistication du jeton d'impact en tant qu'instrument financier.

Le protocole IXO permet en outre de monétiser les données générées par le token d'impact, en tirant parti des marchés de données basés sur la blockchain, comme celui que propose le **protocole Ocean**. Le protocole Ocean[97], fondé par Bruce Pon du MIT en 2017 et aujourd'hui basé à Singapour, est associé au Forum économique mondial et au Media Lab du MIT. Ocean Protocol, par le biais de jetons ERC-20, est un écosystème permettant à n'importe quelle organisation de partager des données, tout en gardant le contrôle et la propriété sur ces dernières, notamment grâce à des algorithmes d'intelligence artificielle reposant sur l'apprentissage fédéré[98].

Ces jeux de données sont disponibles sur l'Ocean Market, où ils peuvent être achetés puis consommés ou vendus. *Via* l'Ocean Protocol, chaque service de données est représenté par un token de données (*data token*) unique, utilisé pour « envelopper »

96 *Ibid.*
97 Ocean Protocol: https://oceanprotocol.com/
98 « Plutôt que de centraliser les données pour y entrainer un algorithme central, l'apprentissage fédéré consiste à entraîner un algorithme sur la machine des utilisateurs d'une application et à partager ensuite les

un jeu de données ou un service « *compute-to-data* » (service permettant d'exécuter des calculs sur ses données) — qui permettent à des tiers d'effectuer des opérations sur ces données sans qu'elles aient à quitter l'enclave sécurisée de l'éditeur[99].

Le protocole Ocean tout comme le protocole IXO amorcent cette nouvelle économie de la donnée dont l'accès, les échanges et la monétisation sont basés sur des protocoles blockchains.

Tout comme le projet **Proof of Impact.** Créé en 2019 à Amsterdam aux Pays, Proof of impact a son siège social à San Francisco aux Etats-Unis. Fleur Heyns, co-fondatrice de la *startup* explique en ces termes la problématique à laquelle l'entreprise son entreprise souhaite répondre : « *comment les entreprises rendent-elles compte de l'impact qu'elles ont ? Comment les consommateurs peuvent-ils discerner les entreprises qui ont un impact positif sur l'environnement de celles qui se contentent de prétendre avoir un impact, dans le cadre d'une tendance insidieuse et omniprésente de* "lavage d'impact" *? Comment les investisseurs peuvent-ils comparer une entreprise avec une autre lorsqu'il s'agit d'évaluer leur valeur à travers une lentille holistique ?*[100] ».

La proposition de valeur de Proof of impact est ainsi de capter à la source des données à partir d'un référentiel de mesures d'impact auprès des entreprises *via* la plateforme Proof of Impact. « *Lorsque ces données sont poussées vers* Proof of Impact*, chaque unité de sortie est automatiquement vérifiée, à l'aide de techniques algorithmiques permettant de s'assurer que les données sont uniques et non anormales. Une fois que les données soumises sont vérifiées, elles sont inscrites dans la blockchain utilisée par Proof of Impact, représentant un «*jeton d'impact*» qui est sécurisé, immuable et vérifiable »*. L'entreprise prévoit, à terme, d'interfacer leur plateforme propriétaire avec la blockchain Ethereum et une blockchain de deuxième niveau.

apprentissages ainsi réalisés » in « Apprentissage fédéré : une nouvelle approche de l'apprentissage machine », Yann Bocchi, 11 août 2021, https://blogs.letemps.ch/yann-bocchi/2021/08/11/apprentissage-federe-une-nouvelle-approche-de-lapprentissage-machine/

99 Ocean Protocol: https://coinmarketcap.com/fr/currencies/ocean-protocol/

100 « Abbreviated White Paper — Proof of Impact », Fleur Heyns, January 26, 2021 https://medium.com/proofofimpact/abbreviated-white-paper-proof-of-impact-89096c307204

Hiveonline a été créé en 2016 à Copenhague au Danemark par Sofie Blakstad pour se concentrer, dès 2019, sur les marchés ruraux africains. Hiveonline « *collecte des actifs numériques tels que des contrats, des paiements, des photographies, des certificats et des garanties, puis les enregistre dans une blockchain accessible à tous les participants au système* ».

L'entreprise, fortement impliquée auprès des ONG et Organisations internationales, dont notamment le Programme des Nations unies pour le développement (UNDP), le Fonds d'équipement des Nations unies (UNCDF), Save the Children ou encore Mercy Corps, a développé trois services complémentaires, tous adossés à des registres distribués afin de répondre au constat que « *partout, les petites entreprises rencontrent les mêmes problèmes pour établir la confiance, accéder au crédit et atteindre les marchés de manière efficace*[1] ».

Le premier service, concerne la dématérialisation de « l'assistance en espèces et sous forme de bons » (Cash and voucher assistance - CVA), largement utilisée par l'aide humanitaire puisqu'elle représente, en 2019, 5,6 milliards de dollars, deux fois plus qu'en 2016, soit 17,9 % de l'aide humanitaire totale[2]. Malgré cette rapide expansion, l'assistance en espèces et sous forme de bons se heurte à un certain nombre de problèmes dont notamment le coût de leur mise en œuvre dès lors qu'il s'agit de distribuer des cartes physiques ou des bons en papier et dès qu'un partenaire financier traditionnel est impliqué (banque internationale, banque locale, opérateur de télécommunication), qui prélève d'importantes commissions à chaque mouvement d'argent.

De plus, il est complexe de savoir qui bénéficie réellement de l'assistance. Sur le terrain, **Hiveonline** explique également « *que de nombreux détaillants n'acceptent pas les bons, car ils ne peuvent pas être certains du remboursement* ». Le système proposé par **Hiveonline** permet de dématérialiser l'assistance en espèces et sous forme de bons qui prennent la forme de token générés *via* la blockchain de Hiveonline, ce qui permet de considérablement réduire le temps de distribution et les coûts de transaction tout en améliorant le suivi, l'évaluation et l'auditabilité du programme d'aide.

Le deuxième service déployé par Hiveonline, **vsla.online,** concerne « *l'accès au crédit, à l'assurance et à l'épargne à un prix abordable pour les communautés de l'économie*

1 « Sustainable Digital Finance for the next billion », Hivenetwork, Hivenetwork website, retrieved May 10 2022, https://www.hivenetwork.online/
2 « The State of the World's Cash 2020 », José Jodar, Anna Kondakhchyan, Ruth McCormack, Karen Peachey, Laura Phelps, Gaby Smith, CalpNetwork website, Jul 23 2020, calpnetwork.org.

informelle[3] ». Selon Sofie Blakstad « *au Niger, il y a plus de personnes, principalement des femmes, dans les réseaux d'épargne informels - 800 000 - que dans l'ensemble du système bancaire formel, qui n'en compte que 700 000*[4] ». L'utilisateur type de l'application Hiveonline au Niger est « *une femme qui n'a fréquenté qu'une année d'école et ne sait ni lire ni écrire, qui n'a jamais utilisé de technologie, qui n'a pas accès à l'électricité ou à l'eau courante et qui fait vivre cinq à quinze membres de sa famille en vendant des produits localement*[5] ».

Le service apporté par Hiveonline consiste en la dématérialisation de programmes du type Village Savings and Loan Associations (VSLA), qui peuvent également exister sous d'autres formes comme les Savings and Internal Lending Communities (SILC) ou encore les tontines, associations regroupant des membres d'un clan, de familles, de voisins ou de particuliers, qui mettent en commun des biens ou des services au bénéfice de tout un chacun à tour de rôle[6]. Ces communautés, en utilisant les outils de Hiveonline, enregistrent l'ensemble de leurs transactions, simplifiant la tenue des dossiers, la sécurité des opérations et garantissant l'identité de chacun des membres. Ces communautés développent alors une forme de réputation financière : « *Au fur et à mesure que ces transactions s'accumulent et sont enregistrées sur la blockchain de Hiveonline, les groupes d'épargne renforcent leur réputation et leur solvabilité en créant un registre numérique des engagements pris et tenus, y compris les prêts et les remboursements au niveau du groupe et des membres individuels*[7] ».

Cette réputation financière permet ensuite à ces communautés d'établir des liens avec des institutions financières de microfinance, plus enclines à prêter, la transparence réduisant le coût et le risque des prêts qu'ils octroient à ces entreprises informelles et ces groupes d'épargne, qui peuvent ainsi diversifier leurs moyens de subsistance et accroître leur accès aux crédits et financements.

Enfin, le troisième service déployé par Hiveonline, myCoop.online[8], promeut le regroupement des agriculteurs sous la forme de coopératives afin de faciliter leur accès à des financements. Selon Sofie Blakstad, « *les petits exploitants agricoles sont piégés dans une pauvreté générationnelle parce qu'ils ne peuvent pas accéder au crédit pour améliorer le rendement de leurs cultures. Les*

3 « A digital solution for savings groups: vsla.online », Hive Network, https://www.hivenetwork.online/rethinking-vsla-community-finance/
4 *Ibid.*
5 *Ibid.*
6 Définition du philosophe et sociologue Zygmunt Bouman.
7 « Building Credit History through Financial Reputation », Hivenetwork, Hivenetwork website, retrieved May 10, 2022, https://www.hivenetwork.online/financialreputation/
8 « Enhancing agricultural cooperatives and rural livelihoods: myCoop.online », retrieved May 13, 2022, https://www.hivenetwork.online/agricultural-cooperatives/

marchés sont inefficaces et dominés par les intermédiaires. Pourtant, 70 % des terres arables d'Afrique ne sont toujours pas cultivées et le potentiel de croissance est énorme. Les entreprises agricoles sont confrontées à de nombreux défis, notamment les flux de trésorerie, la saisonnalité, la perte de bénéfices au profit des intermédiaires et les catastrophes naturelles[9] ».

En plus de considérablement simplifier la gestion administrative et financière d'une coopérative agricole, le fonctionnement de myCoop.online est le suivant : **Hiveonline** crée d'abord une identité unique pour les agriculteurs de l'association ou de la coopérative (voir chapitre Identité & Propriété). Les agriculteurs publient ensuite des prévisions de récoltes, plantent puis assurent leur livraison, toutes les transactions étant enregistrées *via* le service myCoop.online. Un score de réputation est généré, à l'échelle individuelle et à celle de la coopérative, selon le respect ou non des engagements. Les institutions financières, les acheteurs et les organismes de soutien visualisent, à travers des tableaux de bord accessibles en ligne, « *les candidats aux prêts, à l'achat de récoltes et à la distribution d'intrants agricoles en fonction de leur historique de comportement fiable* ».

Un agriculteur pourra ensuite accéder plus facilement à des prêts, notamment pour l'achat d'intrants agricoles pour démarrer une nouvelle récolte.

Hiveonline s'est associé dès 2019 à l'Association mozambicaine pour la promotion des coopératives modernes (AMPCM) et à la *Royal Norwegian Society for Development* pour le développement d'une solution numérique pour les coopératives. Les premières expérimentations, menées pour apporter une aide aux petits agriculteurs travaillant pour l'industrie de la noix de cajou, se sont depuis développées à d'autres cultures au Mozambique, avec toujours ce même objectif de professionnaliser l'agriculture et d'améliorer les rendements des petits exploitants.

Les défis relevés par Hiveonline sont notamment « *l'absence d'antécédents en matière de crédit ou de réputation financière, afin de prouver aux prêteurs qu'ils sont fiables, l'inefficacité des marchés et la faible productivité due au manque d'accès à des intrants agricoles abordables*[10] ».

9 « Solve, an initiative of the Massachusetts Institute of Technology (MIT): hiveonline, Sustainable digital finance without a phone », retrieved May 13, 2022, https://solve.mit.edu/challenges/digital-inclusion/solutions/48750
10 Hive Network, Agricultural Cooperatives: https://www.hivenetwork.online/agricultural-cooperatives/

ENJEUX ET QUESTIONS

La diversité des enjeux et des questions soulevés par la perte du monopole des États sur la monnaie, ou tout du moins sur le transfert de valeur, révèle combien la société dans son ensemble amorce une transition entre un ancien modèle à bout de souffle et un nouveau modèle, encore en devenir.

Le déclencheur de cette transition coïncide avec l'invention du calculateur universel dans les années 1950, c'est à dire de l'informatique, puis du réseau internet dans les années 1970 et de ses services comme le web ou le mail, puis de leur intrication depuis moins de 15 ans dans une version contemporaine et décentralisée, à la manière dont la blockchain Ethereum se définit elle-même : « *un ordinateur mondial, que n'importe qui peut programmer et utiliser comme il le souhaite. Cet ordinateur est toujours allumé, il est très sécurisé, et tout ce qui est fait à l'aide de cet ordinateur est public*[1] ».

D'innombrables questions restent en suspens à propos de chaque usage et expérimentation qui se développent autour de ces blockchains et de leur *token*.

Envois de fonds transfrontaliers, paiements et micropaiement en pair-à-pair, finance dite décentralisée qui permet d'emprunter, épargner et investir sans établissement bancaire, monnaies locales complémentaires d'un nouveau genre, assurances paramétriques décentralisées, revenu universel, financement participatif, finance inclusive, vérification d'impact ou encore investissement d'impact, il semble que la diversité des initiatives donne à voir l'émergence d'un phénomène destiné à durer.

L'intérêt d'envoyer des fonds transfrontaliers de personne à personne en utilisant des crypto-actifs est indéniable : des transactions quasiment instantanées, des frais réduits, ainsi que l'assurance de posséder ses fonds. Se pose alors la question de savoir comment pourraient se développer des ponts entre l'économie réelle, qu'elle soit informelle ou officielle, dont les échanges s'appuieraient sur cette nouvelle forme d'argent programmable.

Puisque le propre d'une crypto-actif est d'être une monnaie électronique pair-à-pair, le premier frein à leur

1 « Qu'est-ce qu'Ethereum ? », Simon Polrot, Ethereum France, 14 février 2016, consulté le 17 mai 2022. https://www.ethereum-france.com/quest-ce-que-lethereum/

adoption tient à la capacité de tout un chacun de s'en emparer : comment télécharger un portefeuille, comment initier une transaction, comment recevoir ou envoyer des fonds en pair-à-pair ? Les crypto-actifs servent-elles d'instrument pour échapper à la dévaluation d'une monnaie locale, ou de monnaie alternative, utilisable localement, parce qu'acceptée comme moyen de paiement, notamment en satoshi* ?

La Finance décentralisée est-elle réservée à ceux qui en ont les moyens mais n'ont pas accès aux marchés financiers, ou va-t-elle élargir son public ? Qu'en est-il des piratages informatiques ou de l'effondrement de crypto-actifs bancales comme le Terra USD, dont le cours est passé de un dollar à quelques centimes en quelques heures en mai 2022, provoquant la disparition pure et simple des économies et investissements de nombreux petits porteurs, notamment au Pakistan, en Inde, en Argentine ou encore au Nigéria[2] ?

Les monnaies locales complémentaires, les monnaies d'inclusions financières ne sont-elles que l'occasion d'améliorer l'efficacité de ces outils monétaires, ou vont-elles devenir des outils de crypto surveillance, pour le meilleur comme pour le pire ?

A ces questions propres à chacun de ces usages s'en ajoutent d'autres, aux enjeux transverses, et concernent notamment l'impact énergétique des blockchains utilisées, leur capacité à monter en puissance au fur et à mesure de leur adoption, la sécurité des *smart contracts** et des applications décentralisées sans oublier l'incertitude légale et réglementaire que font peser les gardiens du système financier traditionnel sur ces monnaies électroniques pair-à-pair.

Nul ne sait encore la trajectoire exacte de ces projets blockchain, ni la manière dont ils rencontreront leur public, si ce n'est que leur taux d'adoption progresse constamment, notamment dans les pays à la marge du système financier traditionnel et dont les ressortissants sont exclus de la société, parce que sans compte bancaire ou sans identité.

2 « Le Krach a balayé les petits porteurs », Leo Schwartz et Abubakar Idris, *Rest of World* in *Courrier International*, n°1649 du 9 au 15 juin 2022.

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