

ABONNEZ-VOUS À **POUR LA SCIENCE** EN TOUTE LIBERTÉ



FORMULE
INTÉGRALE
-42%



8,20€*

FORMULE
PASSION
-28%



6,50€*

FORMULE
DÉCOUVERTE
-25%



4,90€*

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

☐ OUI, JE M'ABONNE À **POUR LA SCIENCE** EN PRÉLÈVEMENT AUTOMATIQUE, JE CHOISIS MA FORMULE ET JE COMPLÈTE L'AUTORISATION DE PRÉLÈVEMENT CI-DESSOUS.

☐ FORMULE **INTÉGRALE**
12 n° de Pour la Science + 4 Hors-Séries
+ Accès illimité aux archives en ligne depuis 1996

8,20€
Par mois
-42%
IPV8E20

☐ FORMULE **PASSION**
12 n° de Pour la Science
+ 4 Hors-Séries

6,50€
Par mois
-28%
PPV6E50

☐ FORMULE **DÉCOUVERTE**
12 n° de Pour la Science

4,90€
Par mois
-25%
DPV4E90

MES COORDONNÉES

Nom : _____
Prénom : _____
Adresse : _____

Code postal _____

Ville : _____

Tél. Pour le suivi client (facultatif) : _____

E-mail obligatoire : _____@_____

J'accepte de recevoir les informations de **Pour la Science** ☐ OUI ☐ NON
et de ses partenaires ☐ OUI ☐ NON

MANDAT DE PRÉLÈVEMENT SEPA

PAG18485STD

En signant ce mandat SEPA, j'autorise Pour la Science à transmettre des instructions à ma banque pour le prélèvement de mon abonnement dès réception de mon bulletin. Je bénéficie d'un droit de rétractation dans la limite de 8 semaines suivant le premier prélèvement. Plus d'informations auprès de mon établissement bancaire.

TYPE DE PAIEMENT : PAIEMENT RÉCURRENT

Titulaire du compte

Nom : _____

Adresse : _____

Code postal _____ Ville : _____

Désignation du compte à débiter

BIC (Identification internationale de la banque) _____

IBAN _____

(Numéro d'identification international du compte bancaire)

Établissement teneur du compte

Nom : _____

Adresse : _____

Code postal _____ Ville : _____

Date et signature

Organisme Créancier : Pour la Science
170 bis, bd. du Montparnasse - 75014 Paris
N° ICS FR92ZZ426900
N° de référence unique de mandat (RUM)

Merci de joindre impérativement un RIB

Partie réservée au service abonnement. Ne rien inscrire

* Par mois et par rapport au prix de vente en kiosque, l'accès numérique aux archives. Délai de livraison : dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 30/06/2018 en France métropolitaine. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à Pour la Science. Votre abonnement en prélèvement est reconduit automatiquement et peut être interrompu par simple lettre. Photos non contractuelles.

L'ESSENTIEL

> Les banques et les États ont, à bien des égards, échoué à instaurer la confiance des citoyens dans l'économie globale.

> Avec la technologie de la blockchain, les relations de confiance sont établies via des machines et des algorithmes, et non via des intermédiaires humains tels que les banquiers.

> Grâce aux blockchains, on pourrait concevoir des systèmes qui rendent impossibles les abus ou escroqueries, plutôt que de les sanctionner après coup.

> L'utilisation à bon escient des blockchains dépendra *in fine* de la façon dont les logiciels géreront l'identité numérique et les données personnelles.

L'AUTEURE



NATALIE SMOLENSKI
anthropologue culturelle,
responsable de la stratégie
commerciale de l'entreprise
Learning Machine, basée
à New York

La blockchain, instrument de confiance?

La blockchain est un outil informatique qui instaure une confiance au sein du réseau qui l'utilise. Quel sera l'impact social ultime de cette technologie? Tout dépendra de la façon dont nos identités numériques et nos données personnelles seront gérées.

Pour participer à l'économie globale d'aujourd'hui, le commun des mortels doit accepter un marché asymétrique: sa vie est transparente pour les États, les banques et les grandes entreprises, alors que le comportement et les rouages des puissants acteurs de l'économie restent cachés. La frontière entre consommateur et citoyen s'est irréversiblement brouillée.

Cette interaction à sens unique est ce que Shoshana Zuboff, chercheuse en sciences sociales à l'université Harvard, appelle le «capitalisme de surveillance», et il s'agit d'un problème structurel majeur. Les institutions dont la fonction même est d'instaurer des relations de confiance sociale, à savoir les banques et les États, ont, dans de nombreuses parties du monde, failli à cette mission, surtout au cours des trois dernières décennies.

Le krach financier de 2008 et ses conséquences ont donné lieu à une sorte de sentiment ambiant d'impuissance. Parmi les affaires qui ont été portées devant les tribunaux, la plupart ont été jugées en défaveur des petits actionnaires, sans que soient condamnés à des peines de prison les grands banquiers. Cela a achevé de convaincre de nombreux individus

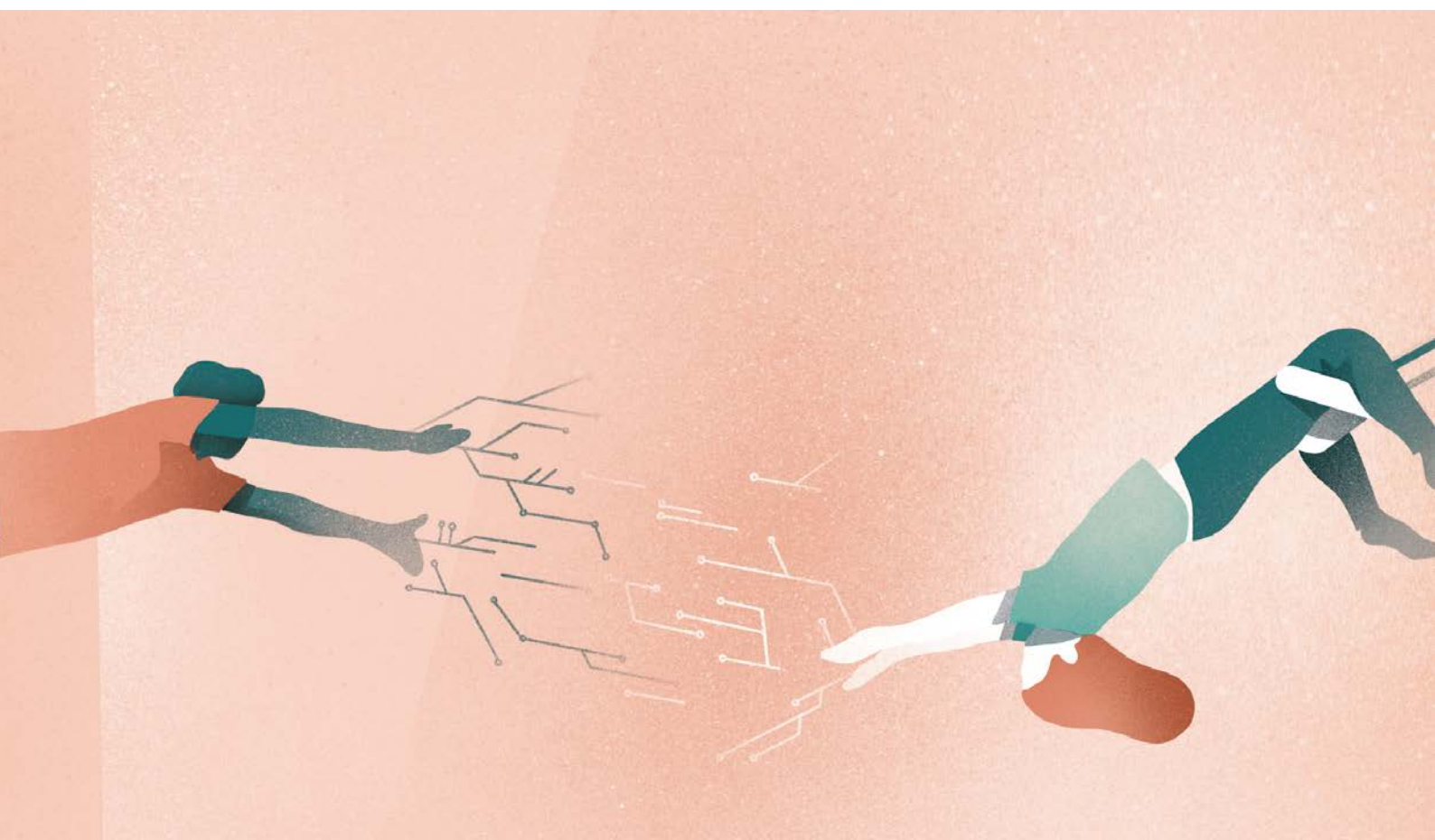
que les riches et les puissants s'associent pour défendre leurs propres intérêts.

Les problèmes vont bien au-delà des retombées liées aux emprunts toxiques. Une analyse d'une base de données de 2007 répertoriant 37 millions d'entreprises et d'investisseurs du monde entier a conclu que 40% de cet ensemble est contrôlé par 1% de ces acteurs, et que le gros de ce 1% est constitué par des institutions financières.

Au cours des trente dernières années, les revenus de placements sont devenus la première source de croissance économique dans la plupart des pays; ils dépassent de beaucoup la croissance des revenus et permettent à la frange la plus riche de s'enrichir toujours davantage. Dans le même temps, 2 milliards d'humains n'ont toujours pas de compte bancaire et sont exclus d'un tissu économique qui, même s'il est loin d'être parfait, est censé faciliter l'accès au capital.

Il n'existe pas de consensus sur la possibilité ou, *a fortiori*, la manière d'infléchir ces tendances pour promouvoir une plus grande inclusion et égalité économique sans nuire à la liberté individuelle. Cela nous amène à un moment historique où les formes d'autorité que sont le pouvoir et la richesse inspirent une méfiance accrue, sur fond d'une vie économique devenue inévitablement globale et mobile. S'il y a bien une tentation de





désengagement et de repli protestataire, il y a aussi la conscience qu'une telle réaction constituerait un autosabotage économique. Ces contraintes ont conduit des technologues du monde entier à imaginer des solutions de remplacement pour établir la confiance à plus grande échelle tout en la rendant plus intime et réciproque. Que la première monnaie numérique prospère, le bitcoin, soit entrée en scène en 2009 n'est pas une coïncidence: cette cryptomonnaie représente une réaction à ce désir croissant de transparence, d'accès et d'autonomisation.

Le bitcoin est une monnaie dont les transactions s'effectuent au moyen d'une blockchain, ou «chaîne de blocs»; il s'agit d'un réseau informatique décentralisé qui consigne dans un registre distribué toutes les transactions préalablement validées par un processus technique de consensus. Les blockchains révolutionnent les possibilités de gestion des échanges directs entre individus, échanges qui peuvent concerner non seulement des sommes d'argent, mais tout bien numérique.

On entend souvent dire que le bitcoin (et les chaînes de blocs en général) ne nécessite pas de confiance. Ce n'est pas tout à fait correct. Plus exactement, la confiance a été retirée aux acteurs humains et transférée à un système cryptographique, avec des incitations

matérielles (gain de bitcoins) à participer au système. En d'autres termes, la confiance est dépersonnalisée.

INSTAURER LA CONFIANCE EN LA DÉSHUMANISANT

De prime abord, cela peut sembler paradoxal. Toutes les formes de confiance ne reposent-elles pas, dans une certaine mesure, sur des humains? Tout au long de l'histoire humaine, la dynamique des migrations et du commerce a conduit à l'élargissement des réseaux de confiance, qui sont passés de petits groupes de personnes connues de tous à des communautés en grande partie constituées d'étrangers et d'adversaires. Pour s'implanter partout sur la planète, nourrir des populations croissantes, mener une guerre, construire des empires ou échanger des savoirs, les gens ont utilisé des techniques de la confiance qui se sont développées les unes à partir des autres, avec un certain recouvrement chronologique: la parenté et le don de cadeaux, la division du travail, la comptabilité (à l'origine du crédit et de la dette), la hiérarchie, la monnaie, les religions universelles et, plus récemment, la banque.

En ce début de ^{xxi}e siècle, la confiance connaît une nouvelle étape de son évolution. Ces mêmes banques qui ont soutenu l'essor du >

> capitalisme moderne en jouant le rôle d'intermédiaires de confiance fiables sont, à bien des égards, devenues un obstacle à son développement. Dans notre système financier actuel, les politiques conduites et les lois visent à décourager les pratiques d'exploitation des individus au moyen de sanctions. À l'avenir, les blockchains pourraient tout simplement être conçues de façon à rendre impossibles ces pratiques.

LES BLOCKCHAINS, UN OUTIL D'ÉMANCIPATION... OU D'ASSERVISSEMENT !

Les règles de consensus du bitcoin, qui fixent les incitations et les exigences encadrant la participation à la blockchain, maintiennent très bien un système de gouvernance distribué, ouvert et pair à pair (voir l'article de John Pavlus, page 28). Ses transactions sont publiques, bien que pseudonymes; le code source du logiciel utilisé est ouvert et maintenu par un réseau global de développeurs bénévoles. De plus, la blockchain du bitcoin ne stocke pas les données d'identification; en guise d'adresses, elle utilise des paires de clés publiques-privées, plutôt que des comptes.

Mais les transactions fondées sur une blockchain sont plus facilement traçables que les transactions en espèces; cela signifie qu'une fois qu'une paire de clés est reliée à une identité connue, l'analyse de la blockchain peut, par exemple, aider la police à retrouver des criminels. Cette réalité va à l'encontre de l'idée répandue selon laquelle les cryptomonnaies conviendraient mieux aux activités criminelles que d'autres types de monnaie.

En fait, les cryptomonnaies réintroduisent le spectre du capitalisme de surveillance. Car les blockchains ont des propriétés qui se prêtent à la fois à l'émancipation humaine et à un degré sans précédent de surveillance et de contrôle. Seront-elles, au bout du compte, au service de notre liberté ou de notre soumission? Tout dépendra de la façon dont le système logiciel, à savoir le protocole de la blockchain et l'application qui lui est adossée, gère les identités numériques de ses utilisateurs.

En ce qui concerne le protocole lui-même, il est important de comprendre qu'il existe plusieurs façons de concevoir une blockchain. Généralement, le terme «blockchain» se réfère à un type de système où un registre de transactions universellement reconnu est répliqué (c'est-à-dire dupliqué et maintenu cohérent sur plusieurs serveurs), mais il n'y a pas d'unanimité sur un ensemble de caractéristiques qu'un tel système doit présenter. D'innombrables modèles de blockchains ont été introduits à ce jour, et ils sont conçus afin d'apporter des solutions à des problèmes différents.

Considérons par exemple Ethereum, une blockchain publique qui se présente comme un

ordinateur distribué global, nommé Ethereum Virtual Machine. Cette blockchain stocke des contrats intelligents qui sont exécutés quand les conditions qu'ils spécifient sont remplies. Son créateur, le Russo-Canadien Vitalik Buterin, envisage que, contrairement au système du bitcoin, les utilisateurs les plus investis dans le réseau (déterminés par des dépôts de garantie en cryptomonnaie) valideront collectivement les nouveaux blocs. Les utilisateurs qui ne respectent pas les règles se verront automatiquement confisquer leur cryptomonnaie.

Certaines blockchains sont conçues pour des communautés où règne entre les membres une grande confiance. Ces blockchains restreintes (*permissioned blockchains* en anglais) reposent généralement sur une autorité centrale qui accorde à des utilisateurs particuliers le rôle de lire ou déposer des transactions. Pour s'assurer que tous les membres de la blockchain se comportent bien, les blockchains restreintes tendent à se reposer sur une autorité centrale plutôt que sur des incitations matérielles automatiques comme dans le système du bitcoin.



Les cryptomonnaies réintroduisent le spectre du capitalisme de surveillance



Un exemple en vue est Ripple, une blockchain conçue pour servir de réseau de règlement lors des transactions interbancaires. De la même façon, l'organisation à but non lucratif EEA (Enterprise Ethereum Alliance) regroupe quelque 200 associés qui construisent une boîte à outils à code source ouvert censé permettre aux entreprises de concevoir leurs propres versions privées de la blockchain Ethereum.

D'autres initiatives similaires sont considérées comme de simples registres distribués, car il leur manque une ou plusieurs des propriétés sous-jacentes des blockchains. Ce sont généralement des registres à accès restreint, où beaucoup de transactions restent privées. L'un des plus importants outils de développement de blockchains privées est R3 Corda, élaboré par un consortium de banques afin de faciliter le consensus concernant les accords financiers.

BIBLIOGRAPHIE

Les nouveaux équilibres de la confiance, entre algorithmes et contrat social, *Cahier de veille de la fondation Mines-Télécom* n° 9, juin 2017 (téléchargeable sur www.imt.fr/cahier-de-veille-confiance-numerique/).

M. Casey et P. Vigna, **The Age of Cryptocurrency : How Bitcoin and Digital Money Are Challenging the Global Economic Order**, St. Martin's Press, 2015.

S. Zuboff, **Big Other : Surveillance capitalism and the prospects of an information civilization**, *Journal of Information Technology*, vol. 30(1), pp. 75-89, 2015.

D. Graeber, **Debt : The First 5,000 Years**, Melville House, 2014.

Les blockchains privées et les registres distribués ont vu le jour en partie pour inclure une forme de contrôle de l'identité des validateurs et de ceux qui effectuent des transactions (par conception, le protocole de la blockchain du bitcoin ne contient pas lui-même de mécanisme de vérification d'identité). L'identité est le terrain sur lequel se jouera le caractère émancipatoire ou oppressif, sur le plan social, des chaînes de blocs. Car plus il est facile de relier les transactions de quelqu'un à une identité (et plus l'identité numérique d'un individu devient centralisée et contrôlée de l'extérieur), plus les possibilités d'abus se multiplient.

DES APPLICATIONS À LA FOIS CONVIVIALES ET DÉPOURVUES DE CONTRÔLE CENTRALISÉ ?

L'individu lambda ne peut pas utiliser directement une blockchain, de la même façon qu'Internet ne peut pas être utilisé directement. En réalité, l'individu utilise des applications qui se servent de la blockchain sous-jacente d'une manière ou d'une autre. C'est dans cette couche d'applications que peuvent régner une grande confusion et, souvent, la mauvaise foi.

L'histoire du système bitcoin, par exemple, est jonchée d'échanges de cryptomonnaie et de fournisseurs de portefeuilles qui ont laissé des failles de sécurité béantes dans leurs applications, ce qui a donné lieu à des piratages retentissants et à des accusations de détournement de fonds.

Dans le cas du réseau Ethereum, des vulnérabilités ont permis le vol ou la perte de millions de dollars de sa cryptomonnaie, l'ether, les utilisateurs lésés n'ayant disposé de pratiquement aucun recours. En général, l'utilisation de n'importe quelle application développée par un tiers auquel on fait confiance pour conserver des biens numériques fondés sur une chaîne de blocs reste une démarche hautement risquée.

C'est là tout le problème insoluble des blockchains : le public ne les utilisera pas s'il ne dispose pas d'applications conviviales. Mais pour être conviviales, les applications recourent souvent à la centralisation, qui reproduit les conditions d'un contrôle centralisé que les blockchains visaient précisément à éviter.

Si l'on veut que les chaînes de blocs deviennent utiles à grande échelle, un certain lien entre l'identité et les transactions sera toutefois nécessaire. Peut-être cette identité n'exigera-t-elle pas de révéler complètement qui vous êtes. Comme l'ont affirmé certains membres de la communauté du bitcoin, la focalisation actuelle sur la vérification de l'identité est en grande partie injustifiée ; en général, ce que les gens veulent savoir, c'est si une affirmation particulière à votre propos est vraie :

avez-vous plus de 21 ans ? Avez-vous réellement obtenu un doctorat au MIT ? Êtes-vous citoyen américain ? Nous avons été habitués par les structures incitatives du capitalisme de surveillance à croire qu'il est nécessaire de livrer une multitude de données personnelles pour suivre notre chemin dans la vie de tous les jours. Changer ce présupposé est l'un des effets les plus radicaux que les techniques de chaînes de blocs pourraient avoir.

Imaginez, par exemple, l'avenir du vote électronique. Une commission électorale doit pouvoir relier une opération de vote à un électeur inscrit afin que cette personne soit notée « a voté ». Mais ce processus n'a pas nécessairement besoin de révéler l'identité de l'individu à la commission : celle-ci pourrait simplement vérifier que le votant est inscrit pour participer à cette élection, et enregistrer qu'il ou elle a voté une fois son choix fait, le tout sans corréler le vote et l'électeur.

Les projets qui minimisent la dissémination de ce qu'on appelle les données à caractère personnel sont encore rares, en partie parce qu'ils ne sont pas faciles à monétiser, que ce soit en devise ou en contrepartie de données personnelles.

Un exemple de projet allant dans ce sens est Blockcerts, une série de bibliothèques de référence gratuites développée par le MIT Media Lab et l'entreprise Learning Machine, où je travaille. Blockcerts permet aux individus de conserver leurs avoirs numériques dans un portefeuille privé hébergé sur leur propre matériel électronique. Les documents communiqués à une personne ne sont associés à aucune identité, à moins que le récipiendaire n'en fasse le choix. Le code source du logiciel est ouvert : on peut donc l'inspecter pour en vérifier l'intégrité et n'importe qui peut l'utiliser en vue de créer ses propres applications pour envoyer, stocker, partager et vérifier des documents officiels. Cette approche est un pas vers ce que certains, dans le domaine de l'identité numérique, ont appelé identité autosouveraine, ce qui signifie que les individus ont le contrôle sur leurs propres données.

Les blockchains sont véritablement une technologie de rupture, qui remet en cause les manières d'envisager la confiance. Mais si les applications s'appuyant sur ces outils ne sont pas conçues dans un souci d'autosouveraineté numérique, rien en principe n'empêchera de traiter les humains comme autant d'objets dans une chaîne logistique, dont chaque mouvement et activité est enregistré, peut-être de façon permanente. Créer des identités numériques dont l'existence soit indépendante des États et des grandes entreprises est le prochain grand défi que nous posent les blockchains – un défi que cette technologie pourrait aussi nous aider à résoudre. ■

L'ESSENTIEL

> Nombre de patients obèses et diabétiques ayant subi une opération gastro-intestinale visant à les aider à perdre du poids ont retrouvé une régulation normale de glucose dans le sang avant même de perdre du poids.

> L'opération consiste à réduire le volume de l'estomac et à

contourner la principale zone d'absorption des nutriments dans l'intestin, le duodénum.

> Le succès de cette approche suggère un lien entre le diabète de type 2 et un dysfonctionnement du tube digestif.

L'AUTEUR



FRANCESCO RUBINO
professeur titulaire de la chaire
de chirurgie bariatrique et métabolique
du King's College London et chirurgien
à l'hôpital du King's College, à Londres

Un scalpel contre le diabète

La chirurgie bariatrique, qui court-circuite certaines parties du tube digestif, se révèle plus efficace contre le diabète de type 2 que les traitements classiques.

Quand j'ai commencé à étudier pour devenir chirurgien, il y a une vingtaine d'années, j'étais impatient de traiter des tumeurs, des calculs, des hernies et d'autres maladies à la portée d'un scalpel. La chirurgie semblait être une solution directe contre bon nombre de maux. Le diabète n'en faisait hélas pas partie. Les opérations concernent une partie précise du corps. Or les médecins savaient que le diabète endommage plusieurs organes en même temps et implique une faille étendue de la régulation de la concentration de glucose dans le sang par une hormone, l'insuline. Le scalpel n'était d'aucune utilité. C'est du moins ce que je croyais jusqu'à un après-midi de l'été 1999, où ma carrière a pris un tournant décisif.

Je venais tout juste de quitter l'Italie pour New York afin de me spécialiser en chirurgie mini-invasive à la faculté de médecine Icahn de l'hôpital du Mont Sinai. Alors que j'étais à la bibliothèque, absorbé dans la lecture des détails techniques de la dérivation biliopancréatique,

une information m'a frappé. Cette opération vise à faire perdre du poids aux patients souffrant d'une obésité sévère en raccourcissant le trajet des aliments à travers l'appareil digestif, de façon à court-circuiter des sections d'absorption des nutriments. Nombre de ces patients avaient un diabète de type 2. Or un mois seulement après l'opération, ces patients avaient retrouvé une glycémie – la concentration de glucose dans le sang – normale. Pourtant, ils n'avaient pas encore perdu beaucoup de poids, n'étaient soumis à aucune restriction de sucre ou de calories, et ne prenaient pas de médicaments contre le diabète. De plus, la plupart n'avaient manifesté aucun signe de la maladie pendant des années après l'opération. Comment une opération pouvait-elle suffire à redonner une glycémie normale dans une maladie connue comme chronique, progressive et irréversible?

Recherchant une explication, je me suis souvenu de l'existence des incrétines. Produites par l'intestin grêle à la suite d'un repas riche en glucides ou en lipides, ces hormones stimulent le pancréas, lequel se met à produire plus d'insuline. Cette dernière favorise le stockage du >