COMPRENDRE LES *BLOCKCHAINS* : FONCTIONNEMENT ET ENJEUX DE CES NOUVELLES TECHNOLOGIES

Valéria Faure-Muntian
Députée

Claude de Ganay
Député

Ronan Le Gleut
Sénateur

ASSEMBLÉE NATIONALE
SÉNAT
LES RAPPORTS DE L'OPECST

Valéria Faure-Muntian
Députée

Claude de Ganay
Député

Ronan Le Gleut
Sénateur

COMPRENDRE LES *BLOCKCHAINS* : FONCTIONNEMENT ET ENJEUX DE CES NOUVELLES TECHNOLOGIES

Valéria Faure-Muntian
Députée

Claude de Ganay
Député

Ronan Le Gleut
Sénateur

Valorisées 250 milliards d'euros, les 1600 cryptomonnaies, dont la principale est le bitcoin, reposent sur la technologie des *blockchains*. Celles-ci assurent le stockage et la transmission d'informations, par la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisés grâce à la cryptographie et structurés par des blocs liés les uns aux autres, à intervalles de temps réguliers.

Les perspectives ouvertes sont considérables. Les applications des *blockchains* dépassent le cadre monétaire même si peu conjuguent, à ce stade, maturité technologique suffisante et pertinence de l'usage. Le recours aux *blockchains* relève encore souvent d'un enjeu de marketing plus que d'une réponse technologique idoine à des besoins avérés.

Les limites actuelles des *blockchains* doivent être identifiées, afin d'encourager des solutions appropriées et pérennes. Plusieurs défis restent à relever par la recherche : capacité à monter en charge, sécurité et, surtout, consommation énergétique. Les questions posées par ces technologies en matière économique et financière, mais aussi juridique ou politique, notamment en termes de souveraineté, sont également sensibles.

En conclusion, le présent rapport plaide pour le développement de *blockchains* européennes qui, sans être souveraines, seraient conçues sur le sol européen, dans le respect de nos principes politiques, philosophiques et moraux. Il convient de s'assurer que la France et l'Union Européenne se saisissent pleinement du sujet des *blockchains* en se plaçant à l'avant-garde de leur développement. Pour l'heure, le choix de la Commission européenne de recourir à une entreprise américaine spécialisée dans la *blockchain* Ethereum pour animer l'Observatoire européen de la *blockchain* constitue un très mauvais signal.

LES RAPPORTS DE L'OPECST

ASSEMBLÉE NATIONALE

SÉNAT

N° 1092

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958
QUINZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale

le 20 juin 2018

N° 584

SÉNAT

SESSION ORDINAIRE 2017 - 2018

Enregistré à la présidence du Sénat

le 20 juin 2018

RAPPORT

au nom de

L'OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES

LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAINES DE BLOCS)

PAR

Mme Valéria FAURE-MUNTIAN, M. Claude de GANAY, députés, et M. Ronan LE GLEUT, sénateur

Déposé sur le Bureau de l'Assemblée nationale

par M. Cédric VILLANI,

Premier vice-président de l'Office

Déposé sur le Bureau du Sénat

par M. Gérard LONGUET,

Président de l'Office

Composition de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

Président

M. Gérard LONGUET, sénateur

Premier vice-président

M. Cédric VILLANI, député

Vice-présidents

M. Didier BAICHÈRE, député
M. Roland COURTEAU, sénateur
M. Patrick HETZEL, député
M. Pierre MÉDEVIELLE, sénateur
Mme Huguette TIEGNA, députée
Mme Catherine PROCACCIA, sénateur

DÉPUTES	SÉNATEURS
M. Julien AUBERT	M. Michel AMIEL
M. Didier BAICHÈRE	M. Jérôme BIGNON
M. Philippe BOLO	M. Roland COURTEAU
M. Christophe BOUILLON	Mme Laure DARCOS
Mme Émilie CARIOU	Mme Annie DELMONT-KOROPOULIS
M. Claude de GANAY	Mme Véronique GUILLOTIN
M. Jean-François ELIAOU	M. Jean-Marie JANSSENS
Mme Valéria FAURE-MUNTIAN	M. Bernard JOMIER
M. Jean-Luc FUGIT	Mme Florence LASSARADE
M. Thomas GASSILLOUD	M. Ronan LE GLEUT
Mme Anne GENETET	M. Gérard LONGUET
M. Pierre HENRIET	M. Rachel MAZUIR
M. Antoine HERTH	M. Pierre MÉDEVIELLE
M. Patrick HETZEL	M. Pierre OUZOULIAS
M. Jean-Paul LECOQ	M. Stéphane PIEDNOIR
M. Loïc PRUD'HOMME	Mme Angèle PRÉVILLE
Mme Huguette TIEGNA	Mme Catherine PROCACCIA
M. Cédric VILLANI	M. Bruno SIDO

S O M M A I R E

Pages

RESUME 11

INTRODUCTION 13

PREMIERE PARTIE : HISTORIQUE ET FONCTIONNEMENT DES *BLOCKCHAINS* 15

I. AUX ORIGINES DES *BLOCKCHAINS* 15

A. UNE INNOVATION TECHNOLOGIQUE DANS LE SILLAGE DU MOUVEMENT POUR LE LOGICIEL LIBRE ET, SURTOUT, DE LA COMMUNAUTE « CYPHERPUNK » 15

1. Le projet d'une monnaie électronique chiffrée permettant de contourner les autorités publiques apparaît dans les années 1980 15

2. Les échecs des premières tentatives de création de monnaies numériques 16

B. L'ARTICLE FONDATEUR DE SATOSHI NAKAMOTO 17

1. Une construction théorique qui vise à relever le défi de la double dépense et celui de la tolérance aux pannes 17

2. La blockchain du bitcoin, un mécanisme de confiance fondé sur des consensus 20

C. LES BLOCKCHAINS PAR RAPPORT A INTERNET 22

1. Le modèle « OSI » 23

2. Une incertitude sur la place des blockchains dans ce cadre 23

II. DES BLOCS « HORODATÉS » RELIÉS PAR LA CRYPTOGRAPHIE : LE FONCTIONNEMENT DE LA CHAINE DE BLOCS 24

A. L'UTILISATION D'ALGORITHMES ASYMETRIQUES 25

1. Un système reposant sur une paire de clés, publique et privée 25

2. Un système pseudonyme plus qu'anonyme 26

3. L'horodatage (timestamping) 26

B. DES BLOCS LIES ENTRE EUX PAR DES FONCTIONS DE HACHAGE 27

1. Le fonctionnement de ces fonctions 28

2. L'utilité du hachage pour la chaîne de blocs 31

3. Les difficultés de ces fonctions 32

III. UN REGISTRE DISTRIBUE MIS À JOUR AU SEIN D'UN RESEAU PAIR A PAIR 33

A. LES NŒUDS DU RESEAU ET LE CONSENSUS 33

1. La diffusion des blocs sur un réseau pair à pair 33

2. La nécessité d'une méthode de consensus 36

B. LA « PREUVE DE TRAVAIL » ADMINISTREE PAR LES MINEURS 37

1. Des épreuves cryptographiques dénommées minage 37

2. La réponse au problème des chaînes parallèles 38

3. La concentration des mineurs 39

C. LES AUTRES MODES DE PREUVES 40

1. La recherche d'alternatives à la preuve de travail 40

2. Les avantages et les inconvénients des différentes méthodes 41

IV. LES REFORMES DES *BLOCKCHAINS* : *HARD FORKS* ET *SOFT FORKS* 43

A. VOIES ET MOYENS DES MODIFICATIONS DU CODE DES BLOCKCHAINS 43

1. Pourquoi modifier le code d'une blockchain ? 43

2. Comment modifier le code d'une blockchain ? 44

B. DES PROBLEMES DIFFERENTS SELON LA RETROCOMPATIBILITE DE LA REFORME 44

1. Distinguer les évolutions selon leur rétrocompatibilité 44

2. Risques et intérêts des hard forks 44

V. DE NOMBREUSES *BLOCKCHAINS* PROPRES A CHAQUE CRYPTOMONNAIE 45

A. LE SYSTEME ETHEREUM ET L'ETHER 45

1. L'ouverture de nouvelles perspectives 45

2. Des problématiques spécifiques 46

3. L'absence de recours au protocole « UTXO » 48

B. LES AUTRES CRYPTOMONNAIES 49

1. Plus de 1 600 cryptomonnaies distinctes en juin 2018 49

2. Quelques exemples 51

VI. LA DISTINCTION ENTRE *BLOCKCHAIN*S OUVERTES OU PUBLIQUES ET *BLOCKCHAIN*S FERMEES OU PRIVEES 53

A. ÉVITER UNE CONFUSION FREQUENTE 53

B. LES BLOCKCHAINS PRIVEES SONT-ELLES DE « VRAIES » BLOCKCHAINS ? 53

VII. LES TECHNOLOGIES DE REGISTRES DISTRIBUES ALTERNATIVES AUX *BLOCKCHAINS* 57

A. DES LEDGERS FONDES SUR DES « GRAPHES ORIENTES ACYCLIQUES » (DIRECTED ACYCLIC GRAPHS OU DAG) 57

1. Des projets en développement 57

2. Des registres distribués qui forment des réseaux maillés 57

B. DES TECHNOLOGIES ENCORE PEU MURES 58

1. Un problème de fiabilité 58

2. Une alternative encore très hypothétique 58

DEUXIEME PARTIE : LES ENJEUX DES *BLOCKCHAINS* 60

I. LES DEFIS DE LA MONTEE EN CHARGE (« SCALABILITE ») ET DE LA SECURITE 60

A. REPONDRE AU DEFI DU NOMBRE DE TRANSACTIONS 60

1. Une question décisive 60

2. Des solutions encore en développement 60

B. REPONDRE AU DEFI DES RISQUES D'ATTAQUES 61

1. Attaques contre les interfaces 61

2. Attaques contre les applications et le cas de TheDAO 61

3. Attaques utilisant le procotole 62

4. Attaques contre le protocole lui même 63

II. D'AUTRES APPLICATIONS QUE LES CRYPTOMONNAIES POUR LA *BLOCKCHAIN* ? 63

A. DES SERVICES D'ATTESTATION ET DE CERTIFICATION GRACE AUX BLOCKCHAINS 65

1. La plupart des applications ne conjuguent pas encore pertinence de l'usage et maturité technologique suffisante 65

2. Les cas de l'Estonie et de Zoug 66

B. L'UTILISATION DANS LES PROCEDURES ELECTORALES ET LE VOTE 67

1. Un cas d'usage encore fragile 67

2. Une analyse du Parlement Européen 68

C. DES SMART CONTRACTS POUR PROGRAMMER LA BLOCKCHAIN 68

1. Une définition encore peu stabilisée 68

2. La réintroduction de « tiers de confiance » 69

D. UN CONTINUUM D'APPLICATIONS ALLANT DE SIMPLES PROJETS AUX APPLICATIONS AVEREES 69

1. Beaucoup d'idées et encore peu de projets concrets 69

2. Les blockchains en sont encore à un stade peu avancé 70

III. LES ENJEUX MONETAIRES, FINANCIERS ET ECONOMIQUES 70

A. UNE VALORISATION DE 250 MILLIARDS D'EUROS 70

1. La place des cryptomonnaies parmi les autres types de monnaies 70

2. Le cas du bitcoin 71

3. Un poids croissant qui reste à relativiser 75

B. LA QUESTION DES ICO (INITIAL COIN OFFERINGS) 76

1. Une des applications phares des blockchains 76

2. Des problèmes allant de la transparence à l'escroquerie 77

3. Une opportunité nouvelle pour le financement des start-up 78

IV. LES ENJEUX ENERGETIQUES ET ENVIRONNEMENTAUX 79

A. PLUSIEURS METHODES D'ESTIMATION 80

1. La méthode économique : 45 à 200 TWh/an 83

2. La méthode « Bévand » : 60 à 80 TWh/an 85

3. La méthode de calcul d'un minimum : 46,5 à 62 TWh/an 86

B. DES IMPACTS CONSIDERABLES, COMME L'ACCROISSEMENT MARQUÉ DES ÉMISSIONS DE GAZ À EFFET DE SERRE 87

C. VRAIES ET FAUSSES SOLUTIONS D'UN PROBLEME QUE LA RECHERCHE DOIT CONTRIBUER A RESOUDRE 90

V. LES ENJEUX JURIDIQUES 91

A. FRAUDES, CADRE JURIDIQUE DEFAILLANT ET REGIME FISCAL FLOU 92

1. Activités frauduleuses 92

2. Insertion de données illégales 93

3. Fiscalité 93

4. Régime de responsabilité 94

B. LA PROTECTION DES DONNEES PERSONNELLES 95

1. La blockchain est-elle compatible avec le RGPD ? 95

2. Quelques solutions techniques envisageables 96

3. Des solutions insuffisantes 97

VI. DES ENJEUX DE SOUVERAINETE ? 98

A. LA GEOPOLITIQUE DU MINAGE 98

B. UNE LOGIQUE MONOPOLITISQUE 98

C. LES PERSPECTIVES EUROPEENNES ET L'IMPASSE DES BLOCKCHAINS SOUVERAINES 99

CONCLUSION 102

LISTE DES PERSONNES CONSULTEES 104

BIBLIOGRAPHIE 106

SYNTHESES DES AUDITIONS CONDUITES PAR LES RAPPORTEURS 110

I. AUDITIONS DU 27 MARS 2018 110

1. Mme Claire Balva, présidente de Blockchain Partner 110

2. M. Renaud Lifchitz, consultant et chercheur en sécurité informatique 115

3. M. Ricardo Perez-Marco, directeur de recherche en mathématiques 119

II. AUDITIONS DU 28 MARS 2018 122

1. Mme Emmanuelle Anceaume, chargée de recherche en informatique (IRISA-CNRS) 122

2. M. Simon Polrot, avocat, fondateur d'Ethereum France et de VariabL 124

3. M. Pierre Porthaux, président de Blockchain Solution et d'EmergenceLab 126

III. AUDITIONS DU 4 AVRIL 2018 130

1. M. Jean-Paul Delahaye, professeur d'informatique à l'Université de Lille I 130

2. M. Manuel Valente, directeur de La Maison du Bitcoin 136

3. M. Gérard Memmi, responsable du département informatique de Telecom ParisTech 139

IV. AUDITIONS DU 24 MAI 2018 143

1. M. Jean Zundel, spécialiste d'Ethereum 143

2. MM. Ken Timsit, directeur général de Consensys France et Jérôme de Tychey, responsable blockchain chez Consensys et président de l'association Asseth 147

3. MM. Nicolas Courtois, professeur à l'University College of London, Vincent Danos, chercheur au département d'informatique de l'École Normale Supérieure et Daniel Augot, chercheur à l'INRIA 150

V. AUDITIONS DU 29 MAI 2018 155

1. MM. Renaud Roquebert, avocat conseil et Bilal Chouli, co-fondateur de Neurochain 155

2. M. David Pointcheval, chercheur au CNRS, ENS/Université PSL – INRIA 160

3. Mmes Amandine Jambert, ingénieur expert à la CNIL, Guilda Rostama, juriste et Tiphaine Havel, conseillère parlementaire 162

4. M. Georg Fuchsbauer, chercheur au département d'informatique de l'ENS 165

REUNION DE L'OFFICE DU 12 AVRIL 2018 : EXAMEN D'UNE NOTE COURTE SUR LES CHAINES DE BLOCS (*BLOCKCHAINS*) 168

REUNION DE L'OFFICE DU 14 JUIN 2018 : ADOPTION DU RAPPORT 178

COURRIER DE LA MISSION D'INFORMATION COMMUNE DE L'ASSEMBLEE NATIONALE SUR LES *BLOCKCHAINS* 189

RESUME

Apparues il y a dix ans comme **combinaisons de technologies plus anciennes formant le protocole sous-jacent au bitcoin**, les *blockchains* permettent des échanges décentralisés et sécurisés, sans qu'il soit besoin d'un tiers de confiance. Plus précisément, elles sont **des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers**.

Leurs applications dépassent le cadre strict des cryptomonnaies et sont **potentiellement nombreuses** mais peu conjuguent, à ce jour, **maturité technologique suffisante** et **pertinence de l'usage**. Devant un certain **phénomène de mode**, un regard plus distancié paraît nécessaire : le recours à la *blockchain* relève souvent d'un **enjeu de marketing** plus que d'une réponse technologique idoine à des besoins avérés.

De plus, certains usages sont **éloignés du projet initial**, surtout s'agissant des *blockchains* privées. Enfin, cet écosystème a fait émerger de nouvelles formes de financement. **Les ICO** (*Initial Coin Offering*), type de levée de fonds original et non-règlementé, rencontrent ainsi un très grand succès (total cumulé de plus de 8 milliards d'euros en mars 2018). Ces émissions d'actifs numériques semblent toutefois peu rationnelles puisqu'elles n'offrent **aucune garantie aux investisseurs** et posent des problèmes de **transparence**, de spéculation, voire d'escroqueries.

Dans ce contexte, la recherche doit encore relever plusieurs défis. Tout d'abord, celui de **la capacité des *blockchains* à monter en charge** alors qu'elles ne permettent qu'un nombre limité de transactions par rapport aux solutions traditionnelles.

Ensuite, celui de la **sécurité de ces systèmes**, loin d'être exempts de failles, en particulier ceux qui offrent les applications les plus élaborées, face à des attaques de différentes natures.

Enfin, et surtout, celui de leur **consommation énergétique**, qui apparaît **totalement excessive**, comprise, selon les estimations, entre 46,5 et 200 TWh/an. Ces besoins sont, en outre, en **augmentation exponentielle** en raison de la « méthode de consensus » la plus fréquemment utilisée, appelée « preuve de travail ». **D'autres méthodes de consensus** doivent être mises en œuvre pour **répondre en urgence à ce défaut majeur**.

Les questions posées par ces technologies en matière **économique** et **financière**, mais aussi **juridique**, notamment en ce qui concerne la **protection des données personnelles**, ou, encore, **politique**, surtout en termes de **souveraineté**, sont également sensibles. La **concentration géographique** des fermes de minage soulève ainsi des questions d'ordre géopolitique. Vos rapporteurs plaident pour le **développement de *blockchains* européennes** qui, sans être souveraines, seraient conçues sur le sol européen, dans le respect de nos principes politiques, philosophiques et moraux. Pour l'heure, le choix de la Commission européenne de recourir à l'entreprise américaine Consensys, spécialisée dans la *blockchain*

Ethereum, pour animer l'Observatoire européen de la *blockchain* constitue un très mauvais signal.

Au total, les **perspectives ouvertes par les *blockchains* sont considérables** et c'est pourquoi leurs **limites technologiques et scientifiques** actuelles doivent être identifiées, afin d'encourager la recherche des **solutions les plus pertinentes et les plus pérennes**. Il convient de s'assurer que **la France et l'Union Européenne** se saisissent maintenant pleinement du sujet des *blockchains* en se plaçant **à l'avant-garde de leur développement**.

INTRODUCTION

Le présent rapport répond à une demande de la mission d'information commune sur « les usages des *blockchains* et autres technologies de certification de registres » créée à l'Assemblée nationale, présidée par Julien Aubert et dont les rapporteurs sont Laure de La Raudière et Jean-Michel Mis.

Il se veut une **contribution aux travaux de cette mission** et complète substantiellement la note scientifique de synthèse publiée par l'Office le 12 avril dernier[1]. Deux autres **travaux parlementaires sont en cours :** d'une part, la commission des finances du Sénat, qui s'intéresse depuis 2014 à ce sujet, essentiellement sur le plan des enjeux monétaires, financiers et économiques des cryptomonnaies, a ainsi conduit à nouveau des auditions en 2018[2], d'autre part, la commission des finances de l'Assemblée Nationale a mis en place une mission sur les cryptomonnaies, présidée par Éric Woerth et dont le rapporteur est Pierre Person. Les travaux de ces deux missions devraient aboutir à la remise de rapports cet été, tandis que la mission d'information commune devrait rendre le sien à l'automne prochain.

Il peut être relevé que le premier colloque sur la *blockchain* réunissant députés, chercheurs et acteurs du secteur a été organisé le 24 mars 2016 à l'Assemblée nationale et s'intitulait « *Blockchain*, disruption et opportunités ». De même, un premier « Forum parlementaire de la *blockchain* », organisé par une société de conseil, s'est tenu le 4 octobre 2016 à la Maison de la Chimie. Il a été suivi d'un deuxième forum le 19 juin 2018.

Ce qu'on appelle, par métonymie[3], chaînes de blocs ou *blockchains* sont des **technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués** (*distributed ledgers*)**, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers**.

Notre regrettée collègue Corinne Erhel, alors députée des Côtes-d'Armor, expliquait à ce sujet dès 2016 qu'il « *faut d'abord bien comprendre comment cela fonctionne, quels sont*

---

[1] *Cf. la note scientifique de l'Office n° 4 : « Comprendre les blockchains (chaînes de bloc) » du 12 avril 2018, consultable sur les sites du Sénat et de l'Assemblée nationale aux adresses suivantes : http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2018_0020_note_blockchain.pdf*

http://www2.assemblee-nationale.fr/content/download/66201/673681/version/1/file/Note_20180412+1859_blockchain.pdf

[2] *Auditions du 7 février 2018 sur les nouveaux usages et la régulation des chaînes de blocs (blockchains) et sur les risques et enjeux liés à l'essor des monnaies virtuelles. En 2014, la commission des finances avait rendu un rapport intitulé « La régulation à l'épreuve de l'innovation : les pouvoirs publics face au développement des monnaies virtuelles » (rapport d'information n° 767, 2013-2014).*

[3] *Au sens strict, une chaîne de blocs est un mode d'enregistrement de données. Cf. la définition donnée par la Commission d'enrichissement de la langue française le 23 mai 2017 : https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000034795042*

les enjeux et les impacts, avant de réguler. Il faut laisser cette technologie se développer, même s'il est vrai qu'elle pose des questions sur la responsabilité et la sécurisation des transactions notamment ».

Pour comprendre le fonctionnement de ces registres informatiques, qui utilisent des **réseaux décentralisés pair à pair** (*peer to peer*) et forment les **technologies sous-jacentes aux cryptomonnaies** (type particulier de monnaies virtuelles[1]), il est nécessaire de revenir à **leurs origines**[2].

Leur mode de fonctionnement particulier permet d'analyser **l'ampleur des enjeux liés à ces technologies**, que ce soit en termes d'**usages**, de **sécurité**, de **consommation énergétique** et d'**impact environnemental** ou encore de **souveraineté**.

---

[1] *Les monnaies virtuelles sont définies par la Banque de France comme des unités de compte virtuelles stockées sur support électronique permettant à une communauté d'utilisateurs d'échanger des biens et des services sans avoir à recourir à la monnaie légale. Ces monnaies n'ont pas de cours légal, ne sont pas régulées par une banque centrale et ne sont pas délivrées par des établissements financiers. La Banque centrale européenne (BCE) en distingue trois : celle des jeux vidéo (existence limitée au cadre du jeu), celle utilisant un flux unidirectionnel (qui peut être achetée avec une devise légale mais ne peut être reconvertie en monnaie légale) et, enfin, celle bénéficiant d'un flux bidirectionnel, comme les cryptomonnaies à l'instar du bitcoin (possibilité de conversion dans les deux sens). Un chapitre du rapport annuel 2018 de la Banque des règlements internationaux fait le point sur la question : « Cryptocurrencies : looking beyond the hype », cf.* https://www.bis.org/publ/arpdf/ar2018e5.pdf

[2] *La compréhension de l'histoire et du fonctionnement de ces technologies peut s'appuyer sur différents ouvrages cités dans la bibliographie qui figure à la fin du présent rapport. Les ouvrages suivants peuvent être relevés : Don et Alex Tapscott « Blockchain Revolution » éditions Penguin Random House ; « Blockchain World », IEEE ; « Blockchain Technology Overview », U.S Department of Commerce ; collectif U « Comprendre la blockchain » ; « La Blockchain décryptée – les clefs d'une révolution » Blockchain France ; Garrick Hileman et Michel Rauchs « Global Cryptocurrency Benchmarking Study » ; Science and Technology Options Assessment (STOA) du service de recherche du Parlement Européen, « How Blockchain technologies could change our lives » ; « Cryptocurrencies : looking beyond the hype », chapitre du rapport annuel 2018 de la Banque des règlements internationaux ; « Les Enjeux des blockchains », rapport de France Stratégie ; Jacques Favier et Adli Takkal-Bataille « Bitcoin » CNRS édition ; Laurent Leloup « Blockchain : La révolution de la confiance », éditions Eyrolles ; Stéphane Loignon « Big Bang Blockchain : la seconde révolution d'internet », éditions Tallandier ; collectif « Bitcoin et Blockchain : vers un nouveau paradigme de la confiance numérique ? » Revue Banque édition ; H.Natarajan, S.Krause et H.Gradstein « Distributed ledger technology and blockchain », Banque mondiale ; « Distributed ledger technology : beyond blockchain », United Kingdom Government Office for Science ; Andreas Antonopoulos « Mastering Bitcoin : programming the open blockchain ». TA-SWISS, fondation suisse pour l'évaluation des choix technologiques, membre du réseau EPTA dont est également membre l'OPECST, rendra prochainement une étude sur la blockchain.*

PREMIERE PARTIE :

HISTORIQUE ET FONCTIONNEMENT DES *BLOCKCHAINS*

I. AUX ORIGINES DES *BLOCKCHAINS*

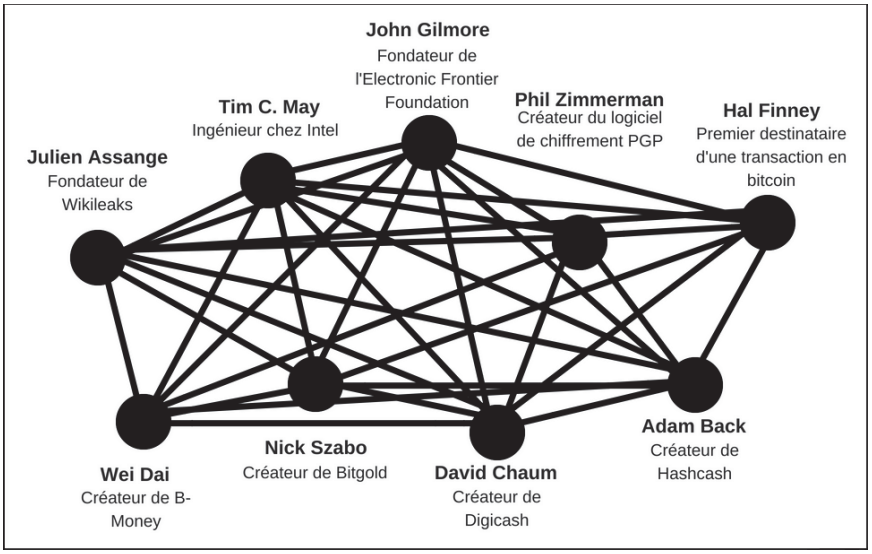
A. UNE INNOVATION TECHNOLOGIQUE DANS LE SILLAGE DU MOUVEMENT POUR LE LOGICIEL LIBRE ET, SURTOUT, DE LA COMMUNAUTE « CYPHERPUNK »

1. Le projet d'une monnaie électronique chiffrée permettant de contourner les autorités publiques apparaît dans les années 1980

L'émergence des cryptomonnaies a partie liée avec le **mouvement pour le logiciel libre**, initié dans les années 1980 par Richard Stallman autour de la Fondation pour le logiciel libre (*Free Software Foundation* ou FSF) et du système d'exploitation libre GNU, ainsi qu'avec la **communauté** « ***cypherpunk*** ». Cette communauté joue un rôle essentiel dans l'écosystème des cryptomonnaies depuis une trentaine d'années.

Le mot-valise « *cypherpunk* », inventé par Jude Milhon à Berkeley en 1992, est formé à partir de l'anglais *cipher* ou chiffrement et « *cyberpunk* », lui-même issu des mots cybernétique et punk et renvoyant à des œuvres de fiction dystopiques basées sur les technologies. Les fondements théoriques de cette mouvance se situent chez Tim May, scientifique alors chargé de la recherche chez Intel, qui publie en 1992 un « *Manifeste crypto-anarchiste* » (*Crypto-Anarchist Manifesto)* et chez Eric Hughes, jeune chercheur à l'université de Berkeley, qui le suit en 1993 avec son « *Manifeste d'un Cypherpunk* » (*A Cypherpunk's Manifesto*). Dans ce contexte, John Gilmore, salarié de Sun Microsystems puis de Cygnus Group et acteur important du *GNU Project* avec Richard Stallman, fonde en 1990 à San Francisco, avec Mitch Kapor et John Perry Barlow, auteur de la « Déclaration d'indépendance du cyberespace », l'*Electronic Frontier Foundation*, véritable annuaire des *cypherpunks*.

Les principaux acteurs de la communauté *cypherpunk*



Source : OPECST d'après Wired

La communauté *cypherpunk* est désireuse d'**utiliser les technologies de chiffrement pour créer une monnaie électronique et garantir des transactions anonymes, contournant ainsi les autorités publiques**, les États au premier chef, mais aussi les banques centrales.

En théorie économique, l'école de Vienne paraît précurseur de cette approche : ainsi Ludwig von Mises explique dès 1912 qu'il « *est impossible de comprendre le principe de la monnaie saine si l'on ne comprend pas qu'il a été conçu comme un instrument de protection des libertés civiles contre les errements despotiques des gouvernements* ».

En 1984, Friedrich Hayek déclare quant à lui : « *je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper* ».

2. Les échecs des premières tentatives de création de monnaies numériques

La théorisation du projet de monnaie électronique fondée sur le chiffrement remonte aux années 1980. Dans un article paru en 1985, au titre évocateur (« *Security Without Identification: Transaction Systems to Make Big Brother Obsolete* »), David Chaum évoque déjà le concept de « cash numérique anonyme » et des protocoles de pseudo-réputation.

Dès 1982, dans l'article « *Blind Signatures for Untraceable Payments* », il avait posé le principe d'un système dans lequel une banque émettrait une unité de paiement, sorte de

« pièce de monnaie signée en blanc »[1]. Cette dernière comprendrait un numéro de série et une signature inconnus, y compris de la banque elle-même. Un tel dispositif devait permettre l'anonymat du client lors d'une transaction, mais aussi l'impossibilité de « retirer » plusieurs fois la même pièce, c'est-à-dire de créer de la monnaie.

En dépit de ces réflexions stimulantes, les **premières tentatives** de création de cryptomonnaies – David Chaum en 1983 avec e-cash puis en 1990 avec digicash, Wei Dai en 1998 avec b-money et, surtout, Nick Szabo avec bitgold – **sont des échecs**.

L'invention de *hashcash* par Adam Back en 1997, avait pourtant marqué un progrès avec l'idée de valider les transactions en utilisant les fonctions de hachage cryptographique, appelées « preuve de travail »[2].

L'objectif de ces technologies est de **rendre inutile l'existence d'un « tiers de confiance »**, en recourant à un système de confiance distribuée permettant de constituer une sorte de « grand livre comptable » infalsifiable.

Cette idée rejoint la définition générale d'une *blockchain* donnée en 2017 par le spécialiste d'ingénierie financière Cyril Grunspan : « *un réseau quelconque où personne ne fait a priori confiance à personne, mais où tout le monde a la possibilité de prouver sa bonne foi* ». Pour certains experts, il s'agit d'un progrès au moins aussi significatif que l'invention de la comptabilité en partie double.

B. L'ARTICLE FONDATEUR DE SATOSHI NAKAMOTO

1. Une construction théorique qui vise à relever le défi de la double dépense et celui de la tolérance aux pannes

Dans les années 1980 et 1990, l'obstacle consistait, dans un cadre décentralisé, à résoudre le **problème de la double dépense**, c'est-à-dire le risque qu'une même somme

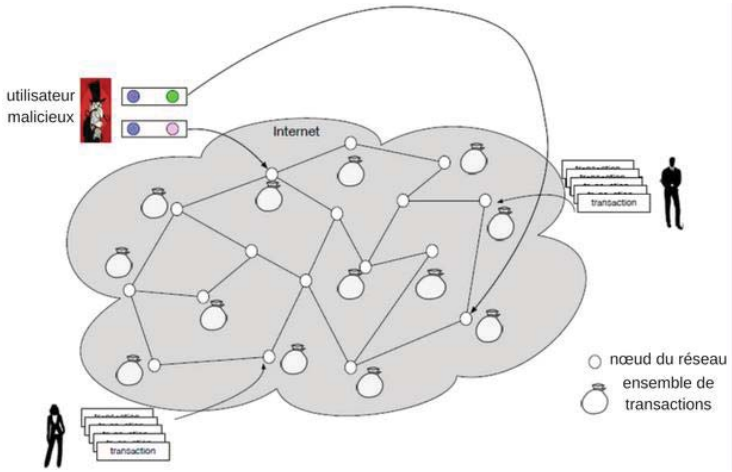
---

[1] *Pour le chercheur Daniel Augot, il convient d'imaginer une enveloppe de papier carbone dans laquelle est insérée une feuille contenant le numéro de série - engendré par l'utilisateur - de la pièce. La banque met alors son tampon sur l'enveloppe sans en voir le contenu (« signature aveugle ») et débite une unité du compte de l'utilisateur. Puis, l'utilisateur sort le papier de l'enveloppe et a obtenu, grâce au papier carbone, un tampon de la banque sur son numéro de série. Il peut ensuite aller faire un achat chez un commerçant, ce dernier accordant sa confiance grâce au tampon de la banque et pouvant ensuite transmettre le papier tamponné à la banque, qui crédite son compte d'une unité. Puisque la banque ne connait pas le numéro de série, elle ignore qui a fait l'achat, ce qui permet de préserver l'anonymat de l'acheteur.*

[2] *Les premières preuves de travail sont apparues dès 1992 avec les travaux de Cynthia Dwork and Moni Naor.*

soit dépensée deux fois et, plus généralement, dans celui de la **tolérance aux pannes**[1], qu'elles soient accidentelles ou malveillantes[2].

Le problème de la double dépense



Source : présentation d'Emmanuelle Anceaume devant l'OPECST

La réponse informatique à ces pannes revient à résoudre le « problème des généraux byzantins » dans le contexte des algorithmes distribués. La tolérance à ces pannes repose donc sur des **techniques dites PBFT** (pour *Practical Byzantine Fault Tolerance*)[3].

---

[1] *Ces problèmes étaient déjà résolus dans un cadre centralisé : en effet, les expériences de e-cash ou de digicash reposent sur des architectures « clients-serveurs » classiques.*

[2] *Cf. Leslie Lamport, Robert Shostak et Marshall Pease «* The Byzantine Generals Problem *», ACM transactions on programming languages and systems, vol. 4, n° 3, juillet 1982.*

[3] *Cf. une liste de publications sur le sujet au lien suivant : http://www.pmg.lcs.mit.edu/bft/*

Le problème des généraux byzantins en informatique

Le problème des généraux byzantins est une métaphore qui traite de la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs. Elle s'applique en particulier au domaine informatique. Un ensemble de composants informatiques fonctionnant de concert doit, en effet, gérer d'éventuelles défaillances parmi ceux-ci. Ces défaillances consisteront alors en la présentation d'informations erronées ou incohérentes. On s'intéresse ici à des problèmes de défaillances, aussi bien matérielles que logicielles, d'origines accidentelle ou malveillante, intervenant pendant l'établissement des informations ou pendant leurs transports d'un composant à l'autre. La gestion de ces composants défectueux est aussi appelée tolérance aux pannes. Ce problème de composants défectueux dans un système informatique peut s'exprimer en termes de généraux byzantins.

Cette notion renvoie à une situation théorique dans laquelle des généraux de l'armée byzantine campent autour d'une cité ennemie. Ils ne peuvent communiquer qu'à l'aide de messagers et doivent établir un plan de bataille commun, faute de quoi la défaite sera inévitable. Cependant un certain nombre de ces messagers peuvent s'avérer être des traîtres, qui essayeront de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille. Il a été démontré que ce problème des généraux byzantins peut être résolu, si et seulement si plus des deux tiers des généraux (messagers) sont loyaux. Ainsi, un seul traître peut tromper deux généraux loyaux.

Source : OPECST d'après Wikipedia

Une des réponses à ces difficultés (double dépense et tolérance aux pannes) est apportée en 2008 dans un **article de Satoshi Nakamoto**.

Derrière ce pseudonyme se cache probablement le collectif des fondateurs du bitcoin et de la première *blockchain*.

Selon plusieurs experts rencontrés par vos rapporteurs, il s'agit d'une équipe pluridisciplinaire, composée notamment de cryptographes de haut niveau, dont plusieurs membres seraient américains[1].

Cet article décrit le fonctionnement d'un protocole permettant la production d'un registre infalsifiable, utilisant un réseau informatique pair à pair – la *blockchain*[2] – comme couche technologique d'une nouvelle cryptomonnaie – le bitcoin.

---

[1] *Satoshi Nakamoto a désigné Gavin Andresen, directeur technique (CTO) de la Fondation Bitcoin, comme étant son successeur. Le fonctionnement de cette cryptomonnaie et de la blockchain est décrit dans un article fondateur publié sur internet en 2008 : « Bitcoin: A Peer to Peer Electronic Cash System », cf. le lien suivant : https://bitcoin.org/bitcoin.pdf et sa traduction en langue française sur le présent lien.*

[2] *Le terme lui-même n'est pas employé dans l'article.*

2. La *blockchain* du bitcoin, un mécanisme de confiance fondé sur des consensus

Il s'agissait donc, à l'origine, de mettre en place un **outil de paiement électronique**, sous la forme de jetons (ou *tokens*), à l'aide d'un réseau décentralisé, autrement dit de créer une **monnaie de l'internet** (le bitcoin) sur le fondement, en quelque sorte et ce n'est qu'une image, d'un « **internet de la monnaie** » (la *blockchain*), créé *ad hoc* et s'appuyant sur les protocoles d'internet sans pouvoir y être assimilés.

Vos rapporteurs relèvent que dans le tout premier bloc créé, appelé *genesis block*, Satoshi Nakamoto a inscrit une suite de chiffres et de lettres qui correspond à la traduction cryptographique d'une courte phrase : « *Times 03/Jan/2009 Chancellor on brink of second bailout for banks* », qui est la une du quotidien britannique « The Times » daté du 3 janvier 2009 et signifie : « *Le ministre des finances britannique au bord d'un second plan de sauvetage pour les banques* ». Pour Pierre Noizat, fondateur de la start-up Paymium qui fait office de banque de bitcoins, « *mettre un titre de journal dans un genesis block, ça permet de dater précisément le lancement. Mais ce titre du Times n'a peut-être pas été choisi au hasard en effet. Il y a cette volonté d'être un contre-pouvoir vis-à-vis des banques* ».

Le calendrier de création du bitcoin a donc également probablement partie liée avec **la crise financière de 2008**, dans le contexte de la crise des *subprimes* et de ses conséquences. En effet, **les questions de confiance dans les banques et les monnaies** étaient alors au centre des préoccupations.

Par ailleurs, selon l'entrepreneur Pierre Porthaux, le bitcoin repose sur **trois consensus interconnectés**, chacun étant nécessaire au fonctionnement général de ce système : un consensus sur les règles, un consensus sur l'histoire et, enfin, un consensus sur le fait que le bitcoin a de la valeur. Pour lui et comme pour toute monnaie, le bitcoin n'a d'ailleurs de la valeur que parce qu'il existe un consensus sur le fait qu'il en a (phénomène de « consensus sur la valeur »). Ces trois consensus ne doivent pas être confondus avec les « méthodes de consensus », qui sont des protocoles au cœur du mode de fonctionnement des *blockchains* et qui feront l'objet de développements spécifiques dans le présent rapport.

Les trois consensus du bitcoin

Source : présentation de Pierre Porthaux devant l'OPECST

Selon Claire Balva, présidente de Blockchain France, le bitcoin s'insère dans un système - la *blockchain* - qui lui garantit certaines qualités précieuses : la résilience, la traçabilité, la désintermédiation et l'intégrité.

Les qualités de la *blockchain* du bitcoin

Source : Blockchain France

La *blockchain* du bitcoin, comme la plupart des *blockchains* qui s'en inspireront ensuite, peut donc être assimilée, au total, à une sorte de **grand livre comptable infalsifiable** qui **rend inutile l'existence d'un « tiers de confiance »**, traditionnellement obligatoire dans les opérations numériques de cessions de titres ou de valeurs. Selon le professeur et chercheur en informatique Jean-Paul Delahaye, il faut, en effet, s'imaginer « *un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible* ». Cette gratuité n'est devenue que relative, du fait des frais de transactions perçus aujourd'hui.

C'est pour cette raison que l'on parle à son sujet d'un **mécanisme de confiance**, *trust machine* comme le titrait *The Economist* en octobre 2015. Grâce à la réputation de cette revue, ce numéro spécial *blockchain* permit alors à cette technologie de sortir du milieu des spécialistes et de se voir conférer une crédibilité dans le grand public, notamment auprès des acteurs économiques.

Un mécanisme de confiance selon *The Economist*

Source : The Economist

Le sous-titre du même numéro de cette revue, « *comment la technologie derrière le Bitcoin pourrait changer le monde* », évoque quant à lui **la révolution potentielle** induite par la *blockchain*. Il s'agirait, selon Salim Ismail, directeur de l'Université de la singularité, de « *la technologie la plus disruptive jamais connue* ».

Un regard plus distancié paraît toutefois nécessaire, en raison des **effets de mode propres aux écosystèmes entrepreneuriaux**. Pour comprendre les impacts des *blockchains*, il faut en effet analyser leur fonctionnement et leurs caractéristiques et savoir tout d'abord les situer par rapports aux réseaux de communication existants tels qu'internet.

C. LES BLOCKCHAINS PAR RAPPORT A INTERNET

La technologie *blockchain* doit être comprise comme **partie intégrante des systèmes informatiques de communication existants**.

En effet, son existence repose sur **le réseau internet et sur ses protocoles**.

Elle présente la particularité d'utiliser un **réseau pair à pair**, c'est-à-dire un réseau au sein duquel chaque internaute peut être serveur ou receveur d'un autre, formant ainsi des pairs dans un modèle décentralisé.

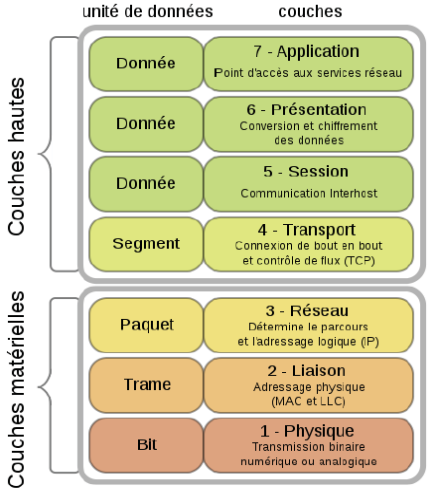
Il est alors envisageable de **la situer par rapport aux autres couches technologiques des systèmes informatiques**.

1. Le modèle « OSI »

Pilier de la théorie des réseaux, le **modèle « OSI »** (*Open Systems Interconnection*) est le standard international ISO de communication en réseau des systèmes informatiques, il représente le modèle basique de référence pour l'interconnexion des systèmes ouverts, norme complète de référence ISO 7498[1].

Les ***blockchains* s'ajoutent à l'ensemble de ces fonctionnalités nécessaires à la communication et à leur organisation**, il convient donc de rapprocher les protocoles des *blockchains* des protocoles à la base du web comme TCP/IP (*Transmission Control Protocol* et *Internet Protocol*) ou HTTP, sans les mettre sur le même plan.

Les sept niveaux de couches du modèle « OSI »



Source : Wikimedia Commons

2. Une incertitude sur la place des *blockchains* dans ce cadre

Une incertitude demeure sur le **niveau de couche sur lequel ou entre lesquels les *blockchain*s viennent se placer**. Elles pourraient se placer entre les couches 3 et 4, ou 4 et 5, mais sans que les experts aient encore déterminé si elles s'apparentent davantage à des couches matérielles ou à des couches hautes, plus applicatives. En effet, les quatre couches inférieures sont plutôt consacrées à la communication et fournies par le matériel et un

[1] *Cf. le texte de la norme ISO 7498 au lien suivant :*

http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

système d'exploitation tandis que les trois couches supérieures sont davantage orientées vers les applications et donc réalisées par exemple à l'aide de bibliothèques ou de programmes spécifiques.

Comme se demande Stéphane Loignon dans son livre « *Big Bang Blockchain* », « *qui, à part les informaticiens, sait comment marchent les protocoles TCP/IP, par lesquels nous transférons les données sur le net, ou http, grâce auquel nous naviguons en ligne ? Nul ne peut pourtant en ignorer ses enjeux, car les usages de cette nouvelle technologie nous concerneront tous. Le web et le courrier électronique ont permis aux individus d'échanger de l'information directement, partout dans le monde et gratuitement (…). La blockchain nous offre la possibilité, pour la première fois, d'utiliser le net pour transférer de l'argent de façon sécurisée, en pair à pair – c'est-à-dire de commercer en ligne sans tiers de confiance* »[1].

Selon Marc Andreessen, fondateur du premier navigateur internet Mosaic puis de Netscape, devenu investisseur de premier plan dans le secteur des technologies de l'information et de la communication (TIC), la *blockchain* fait figure de **révolution informatique comparable aux deux grandes révolutions précédentes : l'ordinateur personnel à partir de 1975 et internet à partir de 1993**[2].

II. DES BLOCS « HORODATÉS » RELIÉS PAR LA CRYPTOGRAPHIE : LE FONCTIONNEMENT DE LA CHAINE DE BLOCS

Le bitcoin repose sur un protocole sous-jacent appelé *blockchain*. On parle de chaînes de blocs, ou *blockchains*, car les transactions effectuées entre les utilisateurs du réseau sont **regroupées par blocs**[3] « **horodatés** ». C'est cet aspect précis de la technologie *blockchain*, objet du présent développement, qui a conduit à donner, par métonymie, son nom à l'ensemble de ces protocoles.

Une fois le bloc validé, en moyenne toutes les dix minutes pour le bitcoin, la transaction devient visible pour l'ensemble des détenteurs du registre, potentiellement tous les utilisateurs, qui vont alors l'ajouter à leur chaîne de blocs. Selon Blockchain France, « *une blockchain est une base de données numérique infalsifiable sur laquelle sont inscrits tous les échanges effectués entre ses utilisateurs depuis sa création* ».

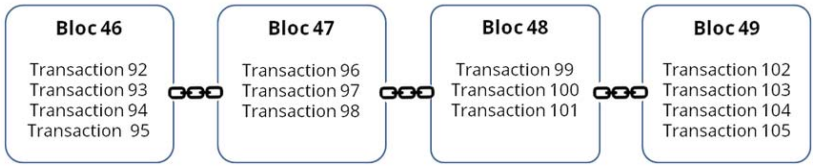
---

[1] *Stéphane Loignon, « Big Bang Blockchain ».*

[2] *Cf. Marc Andreessen, « Why bitcoin matters »,* New-York Times*, 21 janvier 2014.*

[3] *En 1991, Stuart Haber et W. Scott Stornetta furent les premiers à proposer une chaine de blocs permettant l'horodatage : https://link.springer.com/article/10.1007%2FBF00196791*

Représentation d'une chaîne de blocs



Source : Blockchain France

Le protocole de Nakamoto se fonde sur **deux outils cryptographiques** alors déjà connus et étudiés : la signature électronique à clé publique fondée sur des algorithmes asymétriques et les algorithmes de hashage. Tous deux sont des fonctions à sens unique, c'est-à-dire qu'ils peuvent aisément être calculés, mais impossibles à inverser. Ils ont toutefois un fonctionnement et des usages bien distincts.

A. L'UTILISATION D'ALGORITHMES ASYMETRIQUES

1. Un système reposant sur une paire de clés, publique et privée

Chaque transaction a recours à la **cryptographie asymétrique**, proposée pour la première fois par Diffie et Hellman en 1976, et aujourd'hui très répandue pour sécuriser les échanges d'informations car elle permet d'assurer l'origine des données tout en préservant leur confidentialité. Elle fonctionne, pour chaque utilisateur, avec une **paire de clés, l'une privée et l'autre publique**.

Cette paire de clés présente le double intérêt de chiffrer ou de signer un message. Dans le cadre du Bitcoin, seule sa fonction de signature est utilisée.

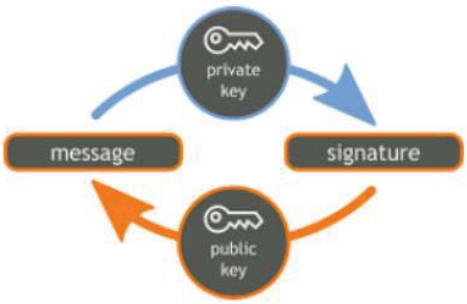
Dans ce système, un utilisateur crée une **suite aléatoire de chiffres, appelée clé privée**. À partir de celle-ci **un algorithme permet de produire une seconde clé appelée clé publique**. Pour le bitcoin, il s'agit d'un algorithme de signature numérique à clé publique dit à courbes elliptiques[1], appelé ECDSA (pour *Elliptic Curve Digital Signature Algorithm*). Par la suite, cette clé privée permettra de signer un message. Les autres utilisateurs du réseau qui connaissent la clé publique correspondante pourront alors vérifier qu'il est bien l'auteur de ce message.

---

[1] *L'ECDSA est inventé en 1992 par Scott Vanstone, en vue de créer un nouveau système de signatures numériques au sein de l'organisme américain de standardisation, le National Institute of Standards and Technology (NIST), cf.* ftp://ftp.iks-jena.de/mitarb/lutz/standards/ansi/X9/x963-7-5-98.pdf

Il s'agit comme l'explique l'article suivant d'une technologie clé pour le bitcoin : https://web.archive.org/web/20160315110426/http://www.e-ducat.fr/bitcoin-2/securite-signatures-ecdsa/

Schéma explicatif de la paire clé publique/clé privée



Source : Wikimedia Commons

Même si elles sont liées de manière unique, **la clé publique ne permet pas de retrouver la clé privée qui en est à l'origine**. La clé publique peut donc être diffusée largement. Ainsi, lors d'une transaction sur le réseau, l'émetteur va utiliser la clé publique du récepteur pour lui transférer un certain nombre de satoshis. Ces derniers représentent la **plus petite fraction de bitcoin**, un **satoshi** équivalent à 0,00000001 bitcoin[1].

Tous les membres du réseau pourront alors lire la transaction et vérifier que l'émetteur était effectivement le dernier possesseur des satoshis envoyés. Seul le récepteur pourra signer la transaction avec sa clé privée pour en prouver la possession.

2. Un système pseudonyme plus qu'anonyme

Sans autre indice, on ne peut identifier le propriétaire d'une clé publique, mais si le lien est fait, on peut alors retracer toutes les transactions qu'il a reçues et envoyées. Le bitcoin est donc un système **pseudonyme** plus qu'anonyme.

La clé publique est diffusable et permet de recevoir des transactions, la clé privée est quant à elle gardée secrète. Seule la clé privée permet d'utiliser les transactions reçues, c'est pourquoi sa préservation est cruciale. En cas de vol ou de perte, il n'existe aucun moyen de récupérer les bitcoins qui ont été envoyés à la clé publique appariée. On estime ainsi qu'entre un cinquième et un tiers de l'ensemble des bitcoins ne sont plus utilisables.

Sans autre indice, on ne peut identifier le propriétaire d'une clé publique, mais dès lors que le lien est fait, on peut retracer toutes les transactions qu'il a reçues et envoyées.

3. L'horodatage (*timestamping)*

Les blocs ainsi constitués de plusieurs transactions « signées » par clés publiques sont ensuite « **horodatés** » (*timestamped*) par leur auteur. Cet aspect, appelé horodatage, est

---

[1] *Un bitcoin est donc équivalent à 100 millions de satoshis.*

essentiel car il permet la **datation relative des blocs** ainsi constitués, la ***blockchain*** formant à cet égard une sorte de chronologie dans laquelle les transactions sont classées les unes après les autres. L'accès à l'historique du registre étant totalement ouvert, les auteurs de tel ou tel bloc peuvent se trouver à n'importe quel point tout autour du globe. Plusieurs blocs pourraient donc être constitués au même moment, de sorte que la même transaction ou deux transactions incompatibles puissent se diffuser de pair à pair.

Le protocole inventé par Nakamoto propose une solution pour limiter le risque qu'une telle production simultanée de deux blocs se produise, et s'assurer qu'un bloc valide ait le temps de se diffuser dans l'ensemble du réseau avant qu'un suivant ne soit créé. Pour la comprendre, il est nécessaire d'évoquer préalablement le fonctionnement des fonctions de hachage.

B. DES BLOCS LIES ENTRE EUX PAR DES FONCTIONS DE HACHAGE

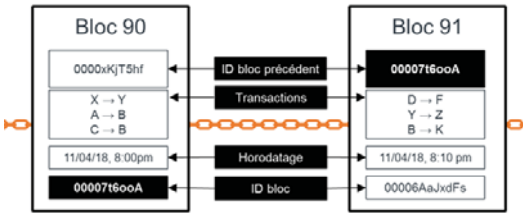
Chaque bloc, outre les transactions et l'horodatage, possède un identifiant (case à fond noir du bloc 90 dans le schéma ci-après), qui prend la forme d'un « hash » permettant de relier les blocs les uns aux autres[1]. Ce hash est toujours le résultat du « hachage » du bloc précédent.

En informatique, les fonctions de « **hachage** » permettent de convertir n'importe quel ensemble de données numériques en un hash, c'est-à-dire en une courte suite binaire qui lui est propre. L'algorithme de compression utilisé à cet effet est appelé « fonction de hachage cryptographique ».

---

[1] *Les arbres de hachage ont été inventés par Ralph Merkle en 1979, d'où l'expression « arbre de Merkle ». Dans le cas du bitcoin ils permettent de réaliser un hash de l'ensemble des transactions d'un bloc, qui est appelé « racine de Merkle » (Merkle Root). L'empreinte de ce bloc résulte alors du hash de cette racine combinée à l'empreinte du bloc précédent.*

La structure d'une *blockchain* et le rôle des hashs



Source : Blockchain France

1. Le fonctionnement de ces fonctions

Le hash d'un ensemble de données peut ainsi être comparé à une **empreinte digitale**, bien moins complexe que l'individu entier, mais l'identifiant de manière précise et unique.

Une fonction de hachage est dite « **à sens unique** » : elle est conçue de telle sorte que le hash produit - à savoir une image ou empreinte de taille fixe créée à partir d'une donnée de taille variable, fournie en entrée - soit impossible à inverser. Alors qu'il est simple de produire un hash à partir d'un ensemble de données, il est **impossible de remonter** à un ensemble de données à partir d'un hash connu, du moins avec les puissances de calcul disponibles aujourd'hui. Cette fonction est donc dite « à sens unique » car l'image d'une donnée se calcule facilement mais le calcul inverse est impossible en pratique.

La conversion des bits en multiplets permet de réduire la longueur d'écriture des lignes de bits, elle est effectuée ainsi :

Binaire	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Hexadécimal	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

À partir d'un ensemble de données au format binaire, la fonction de hachage va effectuer un très grand nombre de manipulations mathématiques relativement simples (remplacement des 0 en 1 ou inversement, combinaison de multiplets…) mais répétées à de nombreuses reprises.

Même si les données de départ représentent un volume très important, la fonction scindera celles-ci en plusieurs tronçons qu'elle combinera par paires, puis rescindera à nouveau jusqu'à obtenir une courte chaîne d'un certain nombre de bits. La longueur de ces hashs est de 256 bits dans le cas de la fonction *Secure Hash Algorithm-256* ou SHA-256, utilisée pour le bitcoin par exemple.

Si l'on applique la fonction SHA-256 au texte complet de la Constitution de la Ve République de 1958, on obtient son hash en base binaire :

01011100 10010000 01011111 00101111 10011010 11010010 10001001 10100101 11110110 11110010 11101100 11110110 10010101 11011110 00100011 10101111 11010001 00011100 00001100 10110101 10010000 10011101 11000101 11100101 01011101 01000010 10011100 00101000 10111111 01010010 11101011 11000001

En base hexadécimale, ce texte s'écrit :

5c905f2f9ad289a5f6f2ecf695de23afd11c0cb5909dc5e55d429c28bf52ebc1

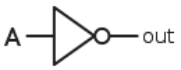
Les transformations apportées par une fonction de hachage

Une fonction de hachage va apporter un grand nombre de transformations à un ensemble de données, quel que soit sa taille, exprimée en langage binaire (0 et 1). Pour cela, elle va utiliser des **portes logiques**, qui sont des outils de base de l'électronique numérique.

Quatre portes logiques, leur signe d'écriture et leur symbole peuvent être présentés :

- La porte « NON », s'écrit ¬ et change les 0 en 1, et inversement.

Exemple : ¬01101=10010



- La porte « ET », s'écrit ∧, et donne 1 pour (1,1) et 0 sinon.

Exemple : 01101∧11000 = 01000

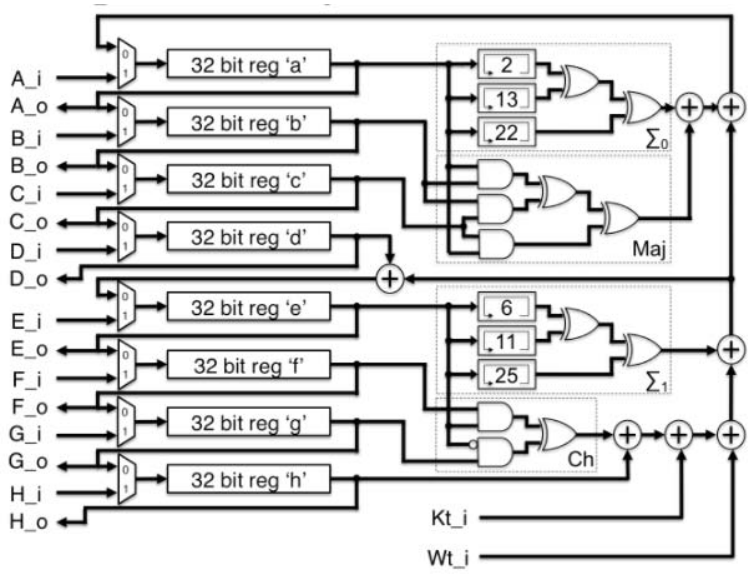
- La porte « OU », s'écrit ∨, et donne 0 pour (0,0) et 1 sinon.

Exemple : 01101∨11000 = 11101

- La porte « OU exclusif » s'écrit ⊕ et effectue une somme bit à bit (où 1+1=0).

Exemple : 01101⊕11000 = 10101

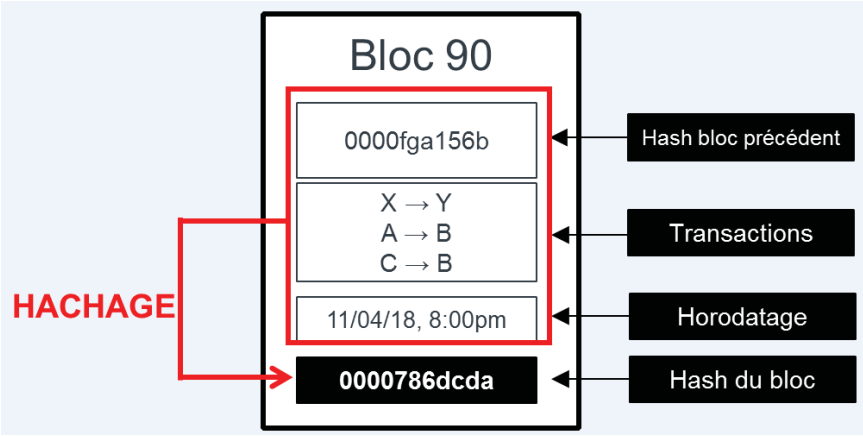
Dans une fonction de hachage telle que SHA-256, ces portes logiques et d'autres opérations vont être appliquées à l'ensemble de données de départ, qui aura été « découpé » en morceaux de 256 bits. Elles se succèdent suivant une organisation complexe répétée une soixantaine de fois, telle qu'illustrée par le schéma suivant.



Source : OPECST d'après Gilles Bailly-Maître et berkeley.edu

Dans le cas d'une chaîne de bloc, le hachage est effectué **à partir du contenu du bloc**, c'est-à-dire le hash du bloc précédent, **un certain nombre de transactions et un horodatage**.

Le rôle des hashs dans les blocs



Source : OPECST

2. L'utilité du hachage pour la chaîne de blocs

La **fonction de hachage SHA-256** est constituée de telle sorte qu'il existe **2^{256} combinaisons possibles** ($1{,}16 \times 10^{77}$), ce qui correspond à l'ordre de grandeur de certaines estimations du nombre d'atomes dans l'univers connu. Le risque de collision, c'est-à-dire de produire deux fois le même hash pour deux ensemble de données différents, revient donc à choisir au hasard deux fois le même atome dans l'ensemble de l'univers connu. On peut ainsi considérer que le hash SHA-256 de chaque ensemble de données est **unique**, avec une très forte marge de sécurité.

Mais le hash est aussi **imprédictible**, que ce soit entièrement ou même partiellement, ce qui est alors considéré comme une « collision partielle » (par exemple pour prévoir la valeur d'un certain nombre de premiers bits). Il est impossible de prévoir quelle valeur aura le hash d'un certain ensemble de données même en ayant connaissance des hashs d'ensembles de données extrêmement proches.

Pour illustrer cette caractéristique notable, on a réalisé un second hash du texte complet de la Constitution en remplaçant simplement le mot « France » par « france » dans la première phrase de l'article premier. Le hash obtenu est alors le suivant :

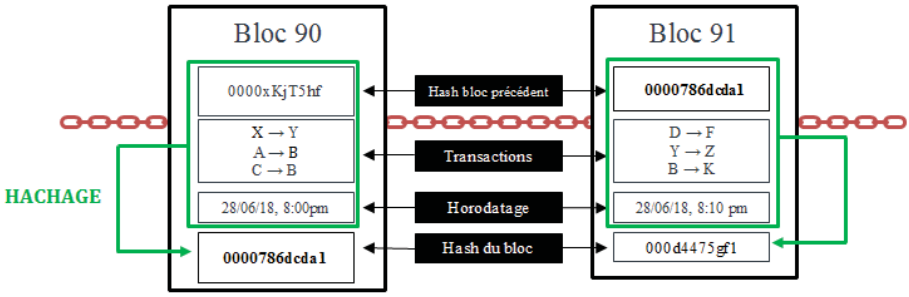
96621d9248e7e2af46b15f8a62b9908a63fc906633cb87aeb966a483e13bba6e

La simple rupture de casse d'une lettre, sur un texte comprenant plusieurs dizaines de milliers de caractères, produit un **nouveau hash ne présentant aucune proximité avec le précédent**.

Cette caractéristique des fonctions de hachage rend **toute modification du contenu d'un bloc immédiatement visible** dans les blocs suivants, même si cette modification est minime. En effet, le hash d'un bloc modifié est nécessairement très différent. Étant donné que ce nouveau hash est intégré au bloc suivant, son hash varie lui aussi. Comme l'indique le graphique ci-après, la modification d'une simple transaction au sein d'un bloc suffit à changer les hashs de tous les blocs suivants.

Le rôle du hachage dans l'intégrité de la chaîne de blocs

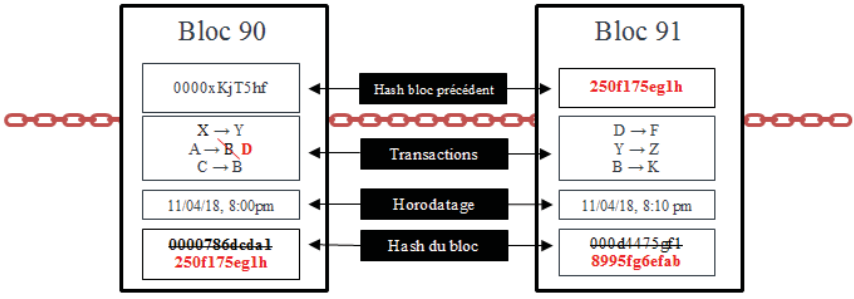
1. Les blocs sont liés par leurs hashs :



Le contenu d'un bloc est soumis à une fonction de hachage pour obtenir son hash (unique et imprédictible)

Ce hash est intégré au bloc suivant, il sera ensuite soumis à une fonction de hachage avec le contenu de ce nouveau bloc pour obtenir un nouveau hash

2. La modification éventuelle d'un bloc est répercutée sur les suivants :



Une **modification du bloc** (ici, le destinataire B remplacé par D) se traduit par un *hash* sensiblement différent

Le *hash* du bloc précédent étant modifié, **le *hash* du bloc suivant est différent** lui aussi, ainsi que le bloc suivant, etc…

Source : OPECST

La modification étant visible dans l'ensemble des blocs suivants, les blocs sont tous liés entre eux cryptographiquement, ainsi que l'a formulé Claire Balva, présidente de Blockchain Partner, devant vos rapporteurs. En conséquence, **modifier le contenu d'un bloc suppose de recalculer les hashs de tous les blocs qui le suivent**.

3. Les difficultés de ces fonctions

Étant donné qu'il demande une **réduction notable de la taille de l'échantillon** et qu'il est **imprédictible**, il est pratiquement impossible de reconstituer un ensemble de données à partir de son hash, ce qu'on appelle une **attaque pré-image**.

La **difficulté des fonctions de hachage doit cependant progresser au même rythme que l'évolution des puissances de calcul informatique**. Ainsi, la fonction *Message digest 5* (MD5) conçue en 1991 n'a plus aujourd'hui qu'une valeur historique, des collisions de ses

« courts » hashs de 128 bits étant désormais trop simples à engendrer pour les calculateurs informatiques actuels.

La fonction utilisée pour le bitcoin se trouve parmi les plus répandues : il s'agit de la fonction SHA-256, vue plus haut, ainsi dénommée car elle produit des hashs d'une taille de 256 bits.

En plus de servir à **lier les blocs entre eux**, ces hashs sont au cœur de la solution proposée par le protocole de Nakamoto pour permettre un **consensus** sur le nouveau bloc à ajouter à la chaîne, à travers une méthode appelée la « preuve de travail ». Cette méthode présente toutefois des limites et d'autres « méthodes de consensus » sont donc envisagées.

III. UN REGISTRE DISTRIBUE MIS À JOUR AU SEIN D'UN RESEAU PAIR A PAIR

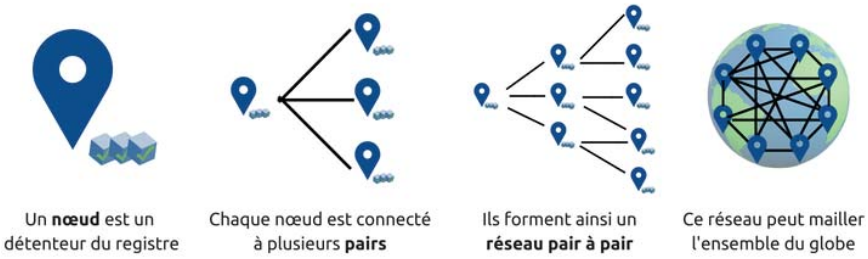
A. LES NŒUDS DU RESEAU ET LE CONSENSUS

1. La diffusion des blocs sur un réseau pair à pair

Chaque bloc est validé par certains utilisateurs baptisés « **mineurs** » (en référence aux chercheurs d'or), et sont transmis aux « **nœuds** » du réseau, c'est-à-dire aux détenteurs du registre, ce registre étant la chaîne de blocs elle-même. Cette dernière est actualisée en permanence.

Dans les *blockchains* dites ouvertes (*permissionless*), comme celle du bitcoin, n'importe quel utilisateur de l'internet peut ainsi devenir un nœud du réseau en téléchargeant le registre auprès d'un nœud existant. Chaque nœud est connecté à plusieurs autres, appelés **pairs**, eux-mêmes ayant leurs propres pairs, ce qui forme un **réseau pair à pair**.

La notion de réseau pair à pair



Source : OPECST

Les nœuds du bitcoin sont **très inégalement répartis dans le monde**, avec près du tiers en Europe et du quart aux États-Unis.

Estimation de la répartition mondiale des nœuds du réseau Bitcoin

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Jun 02 2018 08:48:37 GMT+0200 (CEST).

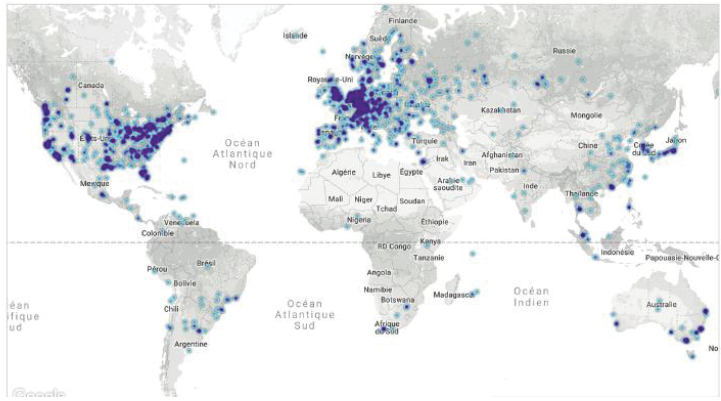
10021 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2479 (24.74%)
2	Germany	1776 (17.72%)
3	China	806 (8.04%)
4	France	654 (6.53%)
5	Netherlands	494 (4.93%)
6	Canada	381 (3.80%)
7	n/a	350 (3.49%)
8	Russian Federation	336 (3.35%)
9	United Kingdom	305 (3.04%)
10	Japan	217 (2.17%)

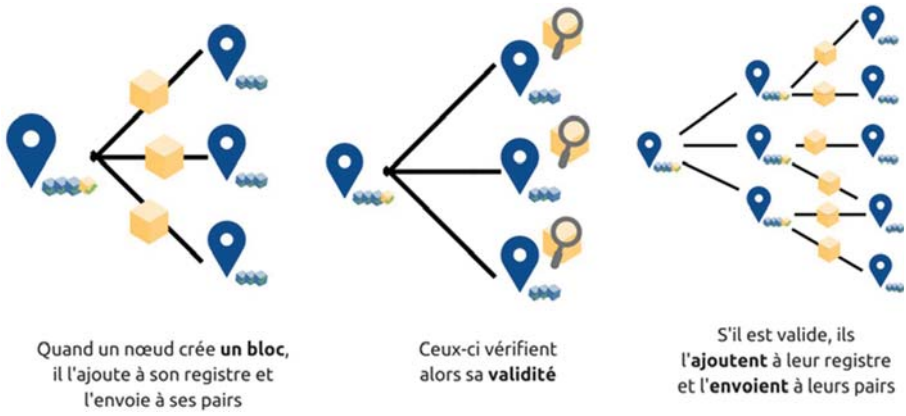
More (104) »



Source : Bitnodes.earn.com

Lorsqu'un nœud crée ou reçoit un nouveau bloc, il l'ajoute à sa copie du registre puis le transmet à ses nœuds pairs. Quand ceux-ci le reçoivent, ils vérifient que ce nouveau bloc est valide, c'est-à-dire qu'ils veillent en particulier à ce que la somme des transactions soit égale en entrée et en sortie. Si le bloc est valide, ils l'intègrent alors à leur registre et le transmettent à leur tour à leurs pairs. À l'échelle planétaire**, «** *il y a forcément une à vingt secondes de latence pour que le bloc se diffuse dans tout le réseau* », selon Bilal Chouli, fondateur de Neurochain.

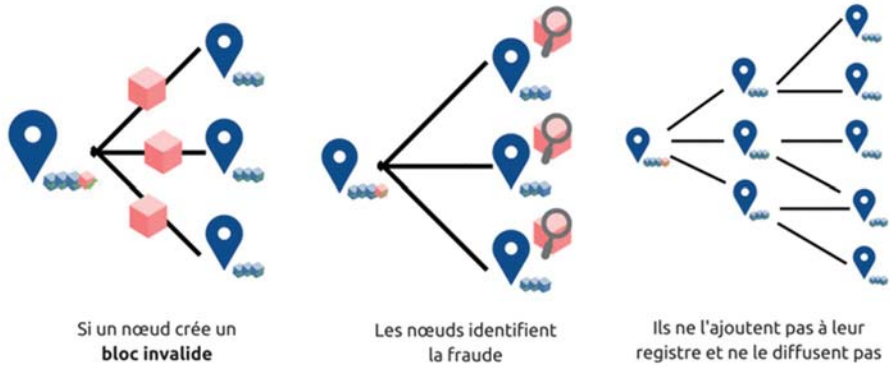
Diffusion d'un bloc dans le réseau



Source : OPECST

Si un nœud essaie d'introduire dans le réseau un **bloc invalide**, celui-ci n'est pas validé par la plupart des nœuds (certains peuvent toutefois être corrompus) et n'est donc pas ajouté à leur registre ni transmis à leurs pairs.

Introduction d'un bloc invalide



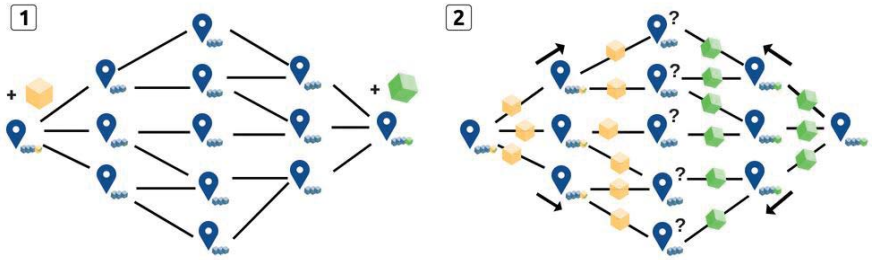
Source : OPECST

La validation des blocs permet donc **de se prémunir du risque d'attaque malveillante**. Aucune autorité centrale ne s'en occupe, puisque les utilisateurs s'en chargent en surveillant le système et en se contrôlant mutuellement. Cette sécurité, source de confiance, est l'un des aspects essentiels de la *blockchain*. Le fait que des centaines de copies du registre soient mises à jour simultanément et régulièrement vise à rendre les *blockchains* **quasiment indestructibles**.

2. La nécessité d'une méthode de consensus

Du fait de l'incompressible latence du réseau évoquée plus haut, plusieurs blocs valides pourraient être créés simultanément par plusieurs nœuds. Les nœuds ajouteraient l'un ou l'autre de ces blocs et le réseau comprendrait alors des registres à des états différents.

Introduction simultanée de deux blocs valides



Deux blocs valides sont émis **par deux nœuds distincts**

Deux versions différentes du registre se diffusent alors sur le réseau

Source : OPECST

Il est donc **nécessaire que les nœuds s'accordent sur le prochain bloc à ajouter à la chaîne**, c'est pourquoi les protocoles de *blockchains* prévoient une « **méthode de consensus** ». En pratique, dans une *blockchain* publique telle que bitcoin, un mécanisme de désignation du bloc validé est utilisé. Son auteur doit fournir la preuve de sa désignation aux autres utilisateurs du réseau.

La méthode la plus simple de désignation consisterait à **tirer au sort** ce validateur, à **intervalle de temps donné** (suffisant pour qu'un bloc puisse se diffuser dans l'ensemble du réseau). Cette solution bute en pratique sur deux obstacles :

- la possibilité de **multiplier les fausses identités** afin de fausser le tirage au sort au profit d'une seule entité (phénomène d'attaques « Sybil »[1]) ;

- l'absence de **temps universellement accepté**, c'est-à-dire d'horloge ne pouvant pas faire l'objet de manipulation malicieuse. Dans un système distribué pair à pair, cette horloge devrait elle aussi être « distribuée ».

Dans le cadre d'une *blockchain* ouverte à tous, une preuve de désignation doit donc présenter deux caractéristiques :

- **empêcher ou rendre difficile la prise en main de la création des blocs par une seule entité** ;

---

[1] *Les attaques « Sybil » reposent sur la multiplication de fausses identités, ce qui peut conduire certains acteurs à exercer une influence disproportionnée sur un réseau. Se prémunir de ces attaques suppose de contrôler la création de profils (validation d'une identité par courriel par exemple) ou, en l'absence d'autorité de contrôle, de produire des calculs informatiques complexes, comme c'est le cas pour le bitcoin.*

- permettre une **temporisation dans la création des blocs**, afin que l'ensemble des nœuds du réseau puissent mettre à jour leur registre.

Le protocole défini par Nakamoto était le premier à proposer une solution relevant ces deux défis, à savoir la **preuve de travail** (*proof of work* ou POW). Dans la mesure où cette méthode de consensus pose des problèmes de diverse nature, d'autres modes de preuves sont donc envisagés comme il sera vu plus loin.

B. LA « PREUVE DE TRAVAIL » ADMINISTREE PAR LES MINEURS

1. Des épreuves cryptographiques dénommées minage

Dans le cas du bitcoin, le mode de validation est une compétition cryptographique appelée « **preuve de travail** » (*proof of work* ou POW). Celle-ci suppose en effet la réussite d'un utilisateur appelé « **mineur** » à une épreuve cryptographique, dénommée « **minage** », qui se répète en moyenne toutes les dix minutes pour le bitcoin. Les mineurs **remportent les nouveaux bitcoins créés** lors de chaque validation de bloc.

La rémunération des mineurs

Le protocole de Nakamoto prévoit que **la création de chaque bloc conduit à l'émission de nouveaux bitcoins**, utilisés pour **récompenser chaque mineur validant un bloc** (qui les reçoit 100 blocs après validation). Le montant de cette récompense est divisé par deux tous les 210 000 blocs, c'est-à-dire tous les quatre ans. Il était ainsi de 50 bitcoins jusqu'en 2012, puis de 25 jusqu'en 2016, il est aujourd'hui de 12,5 et passera à 6,25 en 2020. Cette réduction progressive du niveau d'émission de nouveaux bitcoins est appelée « *halving* ». Elle a pour objectif de maintenir une certaine rareté de cette monnaie.

Les mineurs, en plus d'être rémunérés lors de la réussite à ces épreuves cryptographiques, prélèvent des **frais sur les transactions qu'ils intègrent à chaque nouveau bloc qu'ils créent**. Le montant de ces frais est en théorie déterminé librement par les utilisateurs, mais les mineurs sélectionnant en priorité les plus élevés, ces frais varient, de fait, en fonction du nombre de transactions en attente.

Source : OPECST

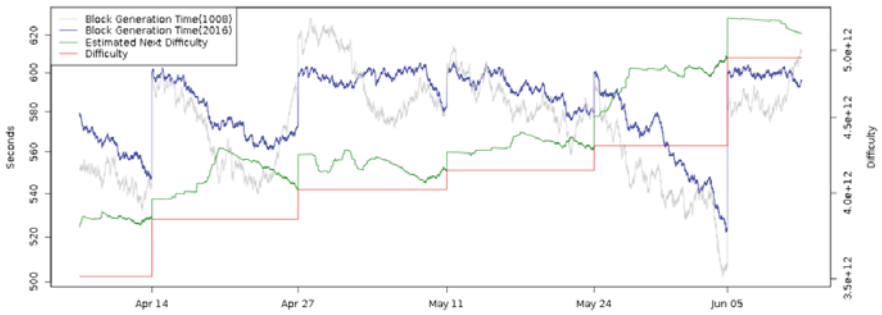
La réussite à l'épreuve consiste à **obtenir un hash** du bloc que le mineur souhaite intégrer, ce hash devant **commencer par un certain nombre de zéros**. Comme il a été vu, une telle opération est très imprédictible et ne peut donc être que le résultat d'un très grand nombre de calculs de la fonction SHA-256. Il s'agit donc d'un **calcul itératif et aléatoire**, dont la résolution peut être **plus ou moins longue** : sa difficulté peut être ajustée de telle sorte que le temps moyen de résolution soit proche d'une durée donnée.

En fonction du nombre de mineurs mobilisés, un hash valide prendra plus ou moins de temps à être trouvé. Afin que les blocs soient **produits à un rythme d'un toutes les dix minutes**, le protocole du bitcoin prévoit par convention un **ajustement régulier de la difficulté**, c'est-à-dire du nombre de zéros exigés. Cette difficulté est ajustée tous les 2 016

blocs, c'est-à-dire environ tous les 14 jours. La difficulté des fonctions de hachage doit en effet progresser a**u même rythme que l'évolution des puissances de calcul informatique**.

Le graphique ci-après illustre cette régulation.

L'ajustement de la difficulté des épreuves cryptographiques



Courbe grise : temps moyen de génération de 1008 blocs
Courbe bleue : temps de moyen de génération de 2016 blocs
Courbe verte : estimation de la difficulté nécessaire au prochain bloc
Courge rouge : difficulté du réseau pour les 2016 prochains blocs
La difficulté est mise à jour **tous les 2016 blocs**, en fonction de l'évolution des temps moyens de génération d'un bloc, afin de **conserver un temps moyen proche de 600 secondes** (10 minutes).
La **différence entre la courbe grise et la courbe bleue** permet d'estimer la dynamique d'évolution de ce temps : plus la courge grise est en dessous de la courbe bleue, plus le temps de génération d'un bloc diminue rapidement. À l'inverse, plus elle est au-dessus, plus ce temps augmente rapidement.

Source : OPECST d'après http://bitcoinwisdom.com/bitcoin/difficulty

2. La réponse au problème des chaînes parallèles

Le bloc validé par le mineur qui sort victorieux des épreuves cryptographiques est alors transmis de pair à pair à chaque nœud qui ajoute à sa propre *blockchain* le bloc ainsi validé. Si deux blocs sont validés au même moment, les mineurs vont utiliser l'un ou l'autre pour intégrer son hash au bloc suivant.

Deux chaînes parallèles se développent alors, des mineurs produisant de nouveaux blocs à partir de blocs ayant des empreintes différentes. Deux mêmes transactions ou des transactions contradictoires pourraient alors être effectuées et transmises aux nœuds du réseau, qui se trouveraient en face d'une contradiction et rejetteraient le dernier bloc reçu.

Le protocole prévoit alors qu'après l'ajout de quelques blocs, seule **la chaîne la plus longue subsiste**, c'est-à-dire en pratique celle que la majorité des nœuds aura adoptée. Les données contenues dans les blocs de la chaîne plus courte ne sont pas valides car elles ne sont pas visibles dans la chaîne gagnante. Elles devront être réémises dans la chaîne la plus longue pour pouvoir être prises en compte.

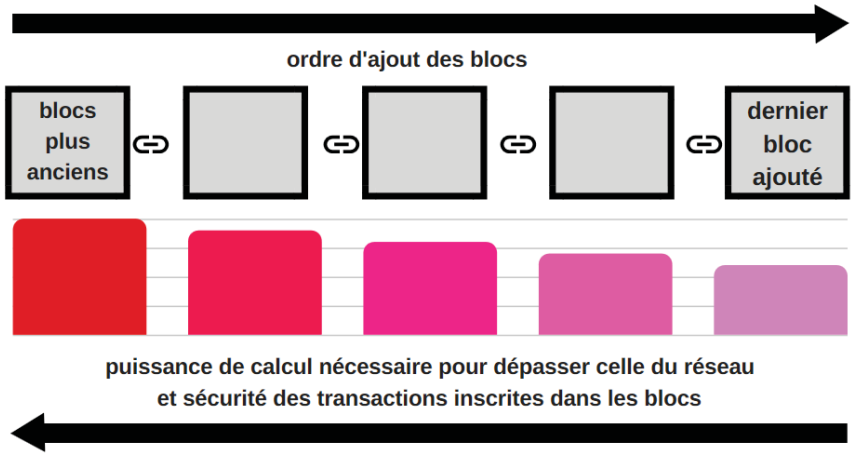
Cette règle s'applique, dans la communauté bitcoin, de telle sorte qu'**après six blocs** (soit une durée d'une heure), des transactions insérées dans un bloc peuvent être considérées comme **validées** et durablement inscrites dans la *blockchain*.

La principale attaque contre l'intégrité d'une *blockchain* consiste donc pour une entité malveillante à produire une chaîne de blocs plus longue contenant des transactions

potentiellement non-valides. Cela suppose qu'elle regroupe suffisamment de puissance de calcul, à un moment donné, pour **dépasser à elle-seule la puissance totale du réseau**.

Cette entité posséderait alors la moitié de la puissance de calcul du réseau, c'est pourquoi on parle d'« **attaque des 51 %** ». La difficulté à attaquer une chaîne est croissante dans le temps, autrement dit plus un bloc est suivi d'autres blocs, moins il va être facile à modifier, comme l'illustre le schéma suivant.

La difficulté croissante dans le temps à attaquer une *blockchain*



Source : OPECST

3. La concentration des mineurs

Les mineurs, rémunérés lors de la réussite aux épreuves cryptographiques et par les frais sur les transactions qu'ils prélèvent, se sont **de plus en plus spécialisés pour optimiser leurs rémunérations et leurs performances**, ce qui conduit à une **concentration** de ces acteurs.

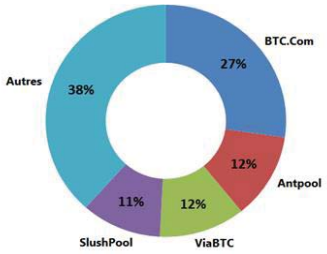
L'**organisation des mineurs en groupements** ou « *pools* »[1] induit le risque qu'une majorité organisée oriente la validation des blocs. La confiance des utilisateurs dans le système étant en théorie un objectif partagé par les mineurs, celui-ci est censé suffire à garantir le respect des règles, dans une logique de « main invisible » protégeant les intérêts privés.

Il faut cependant souligner que quatre *pools* dont trois chinois, appuyés sur des « fermes de minage », assurent aujourd'hui plus de 60 % de la puissance

[1] *L'appartenance à un pool assure des revenus plus constants aux mineurs. Il existe trois pools d'envergure réduite en France : Big Block Data, Wizard Mining et Just Mining.*

de calcul nécessaire à la *blockchain* du bitcoin et pourraient utiliser cette position dominante contre l'intérêt des autres utilisateurs. Selon Nicolas Courtois, il serait possible qu'ils le fassent de manière discrète.

Les « *pools* » de mineurs du bitcoin



Source : Blockchain.info (avril 2018)

La concentration et l'augmentation exponentielle des puissances de minage sont deux défauts souvent reprochés à la preuve de travail, c'est pourquoi beaucoup d'espoirs reposent sur le développement de *blockchains* utilisant d'autres méthodes de consensus.

C. LES AUTRES MODES DE PREUVES

1. La recherche d'alternatives à la preuve de travail

Selon le professeur Jean-Paul Delahaye, « *le problème de la consommation électrique des cryptomonnaies est celui de la preuve de travail* », c'est pourquoi des alternatives sont développées et ont vocation à la remplacer. Cependant, leur sécurité est souvent moins certaine et elles présentent un risque de centralisation.

La principale alternative est appelée preuve d'enjeu ou *proof of stake* (POS). Son principe consiste à attribuer la validation de chaque bloc de manière aléatoire à un utilisateur, selon une probabilité qui n'est pas proportionnelle à une capacité de calcul spécialisée comme c'est le cas pour la preuve de travail.

Cependant pour éviter les attaques par multiplication d'identités (attaques *Sybil*), il est nécessaire que cette distribution aléatoire soit pondérée d'un facteur limitant (exemple : quantité de cryptomonnaies détenue en prenant en compte la durée de détention) ou qu'un mécanisme de sanction soit mis sur pied afin de dissuader la fraude.

La POS recouvre en réalité deux preuves distinctes : la **preuve de participation**, qui consiste à attribuer les blocs en fonction de la quantité de

cryptomonnaies possédée par un nœud, tandis que la **preuve d'enjeu**, en tant que telle, va plus loin en exigeant de mettre en gage ces monnaies, qui seront détruites en cas de fraude.

Selon Sigrid Seibold et George Samman, du cabinet KPMG, la *proof of stake* consiste à « *créer un mécanisme qui punit les nœuds qui ne suivent pas le protocole de consensus* »[1]. Les participants doivent miser un montant prédéfini d'actifs numériques sur le résultat du consensus. Si ce résultat n'a pas lieu, les nœuds malveillants (ceux qui avaient parié contre le consensus majoritaire) perdent leur mise.

Des dérivés de cette preuve d'enjeu existent, on peut citer la « **preuve de possession** » (*proof of hold*), fondée sur la durée de possession, la « **preuve d'utilisation** » (*proof of use*), en fonction du volume de transactions, la « **preuve d'importance** » (*proof of importance*), reposant sur la « réputation », ou encore la « **preuve de destruction** » (*proof of burn*) qui revient à détruire des cryptomonnaies, pour obtenir la confiance du réseau.

Deux autres méthodes distinctes de la preuve d'enjeu, encore à l'état théorique, peuvent aussi être évoquées : la « **preuve de capacité** » (*proof of space*) consiste à mettre en gage de l'espace disque disponible tandis que la « **preuve de travail utile** » *(proof of useful work*) consisterait à utiliser les puissances de calcul du minage à des fins scientifiques, par exemple pour la modélisation de molécules complexes.

La cryptomonnaie peercoin **mélange la preuve de travail et la preuve de participation**, c'est-à-dire qu'elle adapte la difficulté du travail de minage en fonction de la « part » de cryptomonnaie possédée par chacun des mineurs.

Il faut noter ici que les *blockchains* à accès restreint, comme *Ripple*, n'ont pas besoin de preuve de travail car une gouvernance centralisée et la connaissance de l'ensemble des nœuds y permettent une désignation plus ou moins aléatoire du nœud qui validera le prochain bloc. Si cette méthode de consensus peut avoir plusieurs déclinaisons, on la nomme de manière générale « **preuve d'autorité** » (*proof of authority*).

2. Les avantages et les inconvénients des différentes méthodes

Si la *proof of stake* et ses dérivés semblent présenter la **meilleure alternative à la preuve de travail et à sa consommation d'électricité exponentielle**, son déploiement reste lent parmi les *blockchains* les plus importantes. La POS doit encore relever un certain nombre de défis.

---

[1] *Rapport de Sigrid Seibold et George Samman pour KPMG, « Consensus. Immutable agreement for the internet of value », cf. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf*

Toutefois, mesurées en termes de pourcentage de la capitalisation de toutes les monnaies cryptographiques, les **preuves de travail sont passées de 99 % en 2013 à 80 % environ** (en juin 2018).

Le tableau ci-après, réalisé par des chercheurs coréens dans le cadre d'un article recensant l'ensemble des méthodes de consensus existantes, résume les points faibles et forts de trois grandes catégories de modes de preuve.

Avantages et inconvénients de la preuve de travail (POW), de la preuve d'enjeu (POS) et d'une forme hybride des deux modes de preuve

Critères	Preuve de travail	Preuve d'enjeu	Forme hybride entre preuve de travail et preuve d'enjeu
Consommation énergétique	Très importante	Faible	Très importante
Besoin de matériel informatique spécialisé	Très important	Pas nécessaire	Important
Risque de séparation du réseau (*forking*)	Possible, lorsque deux nœuds trouvent le bon hash au même moment	Très improbable	Probable
Vulnérabilité aux attaques des 51%	Existante	Faible	Existante, mais moins que pour la preuve de travail simple
Vitesse de création des blocs	Lente, dépend de plusieurs variables	Rapide	Lente, dépend de plusieurs variables
Risque de regroupement en *pools*	Oui, mais peut être prévenu	Oui, mais difficile à prévenir	Oui
Exemples	Bitcoin	Nextcoin	PPcoin, Blackcoin

Source : OPECST, d'après Giang-Truong Nguyen and Kyungbaek Kim[1]

On peut donc distinguer une méthode fiable et sécurisée, mais lente et coûteuse en énergie, la preuve de travail et une seconde méthode, plus économe tant en énergie qu'en matériel spécialisé, mais à la sécurité encore contestée. Il faut ajouter que la preuve d'enjeu permet également une création beaucoup plus rapide des blocs, donc une capacité plus grande à monter en charge (défi de la scalabilité).

La **sécurité est la première critique** des détracteurs de la preuve d'enjeu, comme Pierre Noizat, qui la considère en effet comme « *prêtant le flanc à une attaque assez simple*[2] ». Les partisans de la preuve d'enjeu relèvent cependant que certains systèmes résistants sont en développement voire fonctionnent déjà sans être attaqués. Parmi les solutions plus résistantes, on peut citer à titre d'exemple le projet Algorand, mené par Silvio Micali, titulaire du prix Turing 2012, dont le fonctionnement correct malgré la présence d'un tiers de nœuds

[1] *Giang-Truong Nguyen et Kyungbaek Kim, «A survey about consensus algorithms used in blockchain », dans le "Journal of Information processing systems", vol. 14, n° 1, février 2018.*

[2] *Pierre Noizat, « Bitcoin, mode d'emploi ». Selon lui, un fraudeur pourrait se procurer à peu de frais des clés de signatures obsolètes à partir des premiers blocs de l'historique des transactions.*

malveillants est prouvé mathématiquement. Le cas de la *blockchain* Cardano, valorisée autour de cinq milliards de dollars en juin 2018 et donc soumise à de fortes pressions sur sa sécurité, peut aussi être mentionné.

La deuxième critique soulève le **risque de capitalisation excessive**, les utilisateurs les plus riches ayant de plus en plus de chances d'obtenir un droit de validation. Cela n'est cependant pas propre à la preuve d'enjeu, comme on a pu le voir avec la formation de *pools* de mineurs.

Enfin, une troisième critique porte sur **la centralisation partielle** qu'entraînerait la preuve d'enjeu, nécessitant un certain contrôle ou une sanction des utilisateurs. Celle-ci semble contraire à l'esprit d'origine des *blockchains*. Il faut noter qu'il s'agit toutefois rarement d'une réelle centralisation, mais plutôt d'une réduction temporaire du nombre de nœuds chargés de la validation, comme c'est le cas avec le protocole *Raft* où sont élus des *leaders* au sein du réseau, chargés de répliquer l'information à ceux qui les suivent.

Toutefois, la preuve d'enjeu est **difficile à mettre en place** et n'a toujours pas été adoptée par les principales *blockchains* telles que Bitcoin, pour laquelle la POS n'avait jamais été envisagée, et même Ethereum, pour laquelle le **passage à la POS** est en revanche prévu depuis l'origine mais a été **repoussé à plusieurs reprises depuis deux ans**. Certains acteurs estiment toujours qu'une *blockchain* ouverte sans sous-jacent physique, c'est-à-dire sans preuve de travail, ne peut fonctionner.

Le **choix d'une méthode de consensus est l'élément déterminant de la gouvernance d'une *blockchain***, de son **niveau de sécurité** et de son **impact**, ce qui explique la prudence des développeurs dans leur mise en place, et des investisseurs dans l'adoption des systèmes qui les utilisent. Paradoxalement, seule une utilisation en conditions réelles les exposant à des attaques importantes permettrait d'identifier de meilleures alternatives à la preuve de travail.

IV. LES REFORMES DES *BLOCKCHAINS* : *HARD FORKS* ET *SOFT FORKS*

A. VOIES ET MOYENS DES MODIFICATIONS DU CODE DES BLOCKCHAINS

1. Pourquoi modifier le code d'une *blockchain* ?

Pour résoudre des *bugs*, s'adapter à de nouveaux usages ou faire face à une croissance du débit des transactions, les règles régissant une *blockchain* doivent pouvoir évoluer. Des blocs seront alors produits sous un nouveau régime de règles, c'est pourquoi on parle d'**embranchement** (« *fork* »).

Étant donné son caractère distribué, toute modification du protocole doit être intégrée dans le code des logiciels détenus individuellement par chaque nœud. Pour garantir l'effectivité de cette mise à jour, un **maximum de nœuds** doit l'adopter.

2. Comment modifier le code d'une *blockchain* ?

Toute personne peut proposer des modifications mais elles émanent le plus souvent de **quelques développeurs** (un noyau d'une quarantaine de personnes dans le cas du bitcoin). Pour le bitcoin, les propositions sont présentées sur la page dédiée au projet sur le site de développement participatif Github. Ainsi il est possible de retracer facilement qui a proposé quelle modification du code et à quel moment.

B. DES PROBLEMES DIFFERENTS SELON LA RETROCOMPATIBILITE DE LA REFORME

1. Distinguer les évolutions selon leur rétrocompatibilité

On distingue **deux types d'évolutions** : les « ***soft forks*** », lorsque les blocs produits sous la nouvelle version peuvent être ajoutés par des nœuds fonctionnant encore sous l'ancienne version, et les « ***hard forks*** », lorsqu'une telle rétrocompatibilité est impossible.

Lorsqu'un *hard fork* n'est pas adopté dans un large consensus, **deux réseaux parallèles** apparaissent alors : l'originel et son alternative. Ils sont **indépendants** dans la mesure où les blocs produits dans une version ne peuvent en général être validés dans l'autre. Des précautions en ce sens sont prises par les développeurs au moment du *fork* car c'est l'intérêt des deux chaînes de **s'assurer que le « divorce » se passe bien**.

En août puis en octobre 2017, **deux modifications du réseau** *Bitcoin Core* ont ainsi échoué à faire consensus. Ayant néanmoins été adoptées par une base suffisante de mineurs, elles ont conduit à la création de deux nouvelles *blockchain*s, respectivement celles de *Bitcoin Cash* et de *Bitcoin Gold*. D'après Manuel Valente, directeur technique de la Maison du Bitcoin, depuis la création du bitcoin, sur 174 propositions de modification, seules 13 ont été acceptées, ce qui témoigne de la dimension assez conservatrice de l'écosystème du bitcoin.

2. Risques et intérêts des *hard forks*

Parce qu'elles font courir un **risque de division de la puissance totale du réseau** et donc un risque de diminution de la confiance en celui-ci, les *hard forks* sont souvent **très contestées**. Certaines réussissent toutefois à faire l'unanimité, la plus emblématique à ce jour restant l'intégration de *Segwit* dans le protocole du *Bitcoin,* fin août 2017, qui a permis d'augmenter le nombre de transactions stockées dans chaque bloc.

Ces *forks* peuvent aussi permettre de **revenir à un état antérieur** de la *blockchain* lorsque celle-ci a été altérée et que l'intégrité du réseau est trop fortement atteinte. Ces *hard forks* « correctrices » ont toutefois pu avoir pour conséquence d'**annuler les transactions ultérieures**, cette réécriture du passé est toutefois contraire à l'esprit des fondateurs des *blokchains*[1].

---

[1] *Ainsi la blockchain zerocoin a corrigé un bug ayant donné lieu au vol de 370 000 unités de cryptomonnaies, pour un bénéfice de 440 000 dollars, sans pour autant être réécrite.*

Le cas de la ***hard fork* de la *blockchain* Ethereum** est probablement **plus emblématique encore**. Elle a eu lieu à la suite d'un hack de l'application **TheDAO** avec pour conséquence la disparition de près de 5 % de la totalité des ethers, monnaie du système Ethereum.

Toutefois, cette *hard fork* a permis de rétablir l'ensemble des transactions échangées sur la *blockchain* depuis l'incident. Cet évènement lié à l'application TheDAO est traité de manière plus détaillée dans la partie du rapport consacré aux risques d'attaques.

V. DE NOMBREUSES *BLOCKCHAINS* PROPRES A CHAQUE CRYPTOMONNAIE

A. LE SYSTEME ETHEREUM ET L'ETHER

1. L'ouverture de nouvelles perspectives

Le protocole Ethereum a été élaboré par **Vitalik Buterin**. En décembre 2013, deux ans après son premier article, ce jeune programmeur russo-canadien de 19 ans publie une description de son projet Ethereum dans le but de lancer des applications décentralisées. Ce projet prend la forme d'un livre blanc, intitulé « Une nouvelle génération de plateforme pour les *smart contracts* et les applications décentralisées[1] ». Pour Claire Balva, présidente de Blockchain France, « *s'il y a une figure à retenir aujourd'hui dans le monde de la blockchain, c'est celle de Vitalik Buterin* ».

Simon Polrot a expliqué que la validation d'un bloc sur Ethereum prend **15 secondes environ**, contre 10 minutes sur Bitcoin mais que « *la différence fondamentale entre les deux grandes blockchains réside dans le langage de programmation : à l'inverse du Bitcoin, celui d'Ethereum utilise un langage Turing-complet (*Turing Complete*)* ».

Un tel système formel possède une **puissance d'expression au moins équivalente à celle des machines de Turing** (caractérisées par la « capacité potentielle de calculer tout ce qui est calculable »), offrant ainsi la possibilité de réaliser des **boucles** et de faire des **fonctions récursives**, ce qui n'est pas possible avec Bitcoin[2]. Ces fonctions s'appellent elles-mêmes dans leur définition, autrement dit leurs valeurs peuvent être calculées en « revenant » sur elles-mêmes.

Le langage de programmation d'Ethereum a donc ouvert de **nouvelles perspectives**, notamment des possibilités d'automatisation d'opérations, mais aussi des **risques plus grands en termes de sécurité** car des *hackers* pourraient programmer un code leur permettant de détourner des ethers de manière répétée.

Pour Nicolas Houy, économiste au CNRS, « *le langage* Turing complete *ouvre la porte aux bugs et aux malwares (programmes malveillants)* ». Pierre Noizat, plutôt partisan du Bitcoin, estime que « *la sécurité est antagoniste de la performance et de la praticité. Il y a une*

---

[1] *Vitalik Buterin, "*A Next-Generation Smart Contract and Decentralized Application Platform"*, décembre 2013. Cf.* https://github.com/ethereum/wiki/wiki/White-Paper *en français :* http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/

[2] *Ce système permet toutefois une programmabilité* a minima *de la monnaie.*

contradiction entre la volonté de faire une machine virtuelle haute performance pour beaucoup d'applications différentes et celle de faire du paiement avec les ethers ».

Selon les promoteurs d'Ethereum cet argument serait fallacieux, Jérôme de Tichey assure ainsi que l'écosystème Ethereum est « *l'une des blockchains les plus robustes, si ce n'est la plus robuste. Bien que la technologie soit jeune, elle avance de façon extrêmement rapide. La plupart des blockchains n'ont pas le soutien nécessaire pour durer ou devenir stables en production. Nous recommandons de ne travailler que sur des plateformes bien établies et soutenues par une communauté* ».

Le langage de programmation d'Ethereum permet l'essor des « *smart contracts* », des programmes qui, en réalité, ne sont ni vraiment des contrats (*contracts*), ni vraiment intelligents (*smart*), sur lesquels le présent rapport reviendra plus tard.

Alors que le protocole du Bitcoin permettait de coder des aspects assez basiques, Ethereum a été conçu pour **dépasser ces limites**, puisque cette *blockchain* lancée il y a trois ans en juin 2015, est selon un expert « *celle qui intéresse le plus les milieux d'affaires, qui voient en elle à la fois une version « politiquement correcte » du Bitcoin, sans l'arrière-fond idéologique anarchiste de la cryptomonnaie originelle, et un outil aux possibilités plus larges* ».

Ethereum permet, de plus, l'émergence de nouveaux modes de collaboration grâce à la baisse des coûts de transaction entre collaborateurs. D'après Vitalik Buterin, il faut voir son système comme un **ordinateur mondial** : ce que Bitcoin permet pour le paiement, Ethereum projette de le faire pour toute chose pouvant être programmée[1].

Le réseau Ethereum est capable d'inclure jusqu'à **1 350 000 transactions par jour** dans le registre, compte une dizaine de milliers d'ordinateurs sur lesquels est répliqué le registre et comprend le solde en ethers de millions de comptes et les codes de plusieurs milliers d'applications.

Depuis 2015, le réseau, sans autorité centrale, n'a toujours pas connu de panne majeure ni de modification pirate, à l'exception de l'attaque notable contre « TheDAO » vue plus loin. Les *smart contracts* comportent le plus souvent leur propre « *bug bounty* » (système de récompenses pour les personnes ayant rapporté des bugs), ce qui permet d'améliorer la qualité du code.

2. Des problématiques spécifiques

Le **passage d'un minage de type *Proof of Work* à un minage de type *Proof of Stake* est prévu**, avec le but de limiter la consommation d'électricité du réseau, mais il est **repoussé depuis deux ans** (systèmes CASPER et Serenity). Cette question épineuse n'est pas encore tranchée par les développeurs. Il faut souligner que le mot mineur ne s'applique que pour les protocoles avec preuve de travail, les autres systèmes de consensus, dont la POS, recourent plutôt aux termes « nœuds participant à la surveillance du réseau » ou « nœuds validateurs ».

Actuellement, le fonctionnement du réseau est donc proche de celui du Bitcoin et en **partage les principales caractéristiques** car il repose encore sur la même méthode de consensus : immutabilité, transparence, infalsifiabilité, réplicabilité... Le défi du passage à la preuve d'enjeu sera de garantir le maintien de ces qualités.

---

[1] *Cf. la citation en anglais : "*Think of Ethereum as a world computer. What Bitcoin does for payments, Ethereum does for anything that can be programmed*".*

Histoire de l'écosystème Ethereum

Source : Ethereum France

Ethereum prévoit un standard pour créer sa propre monnaie ou *token* à l'intérieur de la *blockchain*, appelé ERC20. Depuis juillet 2015, il y a ainsi eu 66 268 *smart contracts* ERC20 déployés sur Ethereum (au 5 avril 2018), ce qui en fait le standard pour les *smart contracts* le plus populaire.

En outre, chaque nœud du réseau exécute l'intégralité des calculs de la machine virtuelle Ethereum (ou EVM). Pour s'assurer que l'exécution d'un code s'achève au terme de chaque opération effectuée (code opération ou OPCODE), il est dépensé une quantité de « gaz » prédéfinie (le gaz est un coût ou une rémunération infinitésimale en ethers). Chaque transaction est constituée d'OPCODE et nécessite donc une certaine quantité de « gaz » (« *Gas Limit* ») : l'utilisateur définit pour sa transaction une quantité de « gaz » nécessaire au traitement de la transaction ; si la limite est dépassée, la transaction est enregistrée mais sans effet. La formule du coût d'une transaction est donc : l'utilisation de « gaz » multipliée par le prix du « gaz » ou « GasUsed x GasPrice (exprimé en ether) ». Comme pour le bitcoin les coûts de transaction sont reversés au mineur qui crée le nouveau bloc.

Ethereum connait des problèmes sérieux en termes de capacité de montée en charge (taille de sa *blockchain*) et de fonctionnement centralisé d'un réseau présenté comme décentralisé. En effet, selon Grégory Guittard « *de moins en moins de nœuds complets valident à l'heure actuelle cette blockchain ETH dans son entièreté (…). Il est théoriquement possible de monter un nœud complet Ethereum sur tout matériel informatique mais dans la pratique les ressources demandées nécessitent un matériel trop coûteux et spécifique pour qu'un opérateur lambda monte un nœud complet aussi facilement que sur Bitcoin, c'est pourquoi la plupart des nœuds complets sont aujourd'hui gérés et entretenus par une seule entreprise privée, Infura* »[1].

Ainsi, **certaines applications** sur le réseau sont susceptibles de **ne plus pouvoir fonctionner lors de pics d'utilisation**. Ce fût par exemple observé avec la première vague de « *crypto-kitties* », cette application de collection et d'échanges de « chats virtuels », plus grand succès à ce jour de la *blockchain* Ethereum, ayant alors totalement congestionné le réseau.

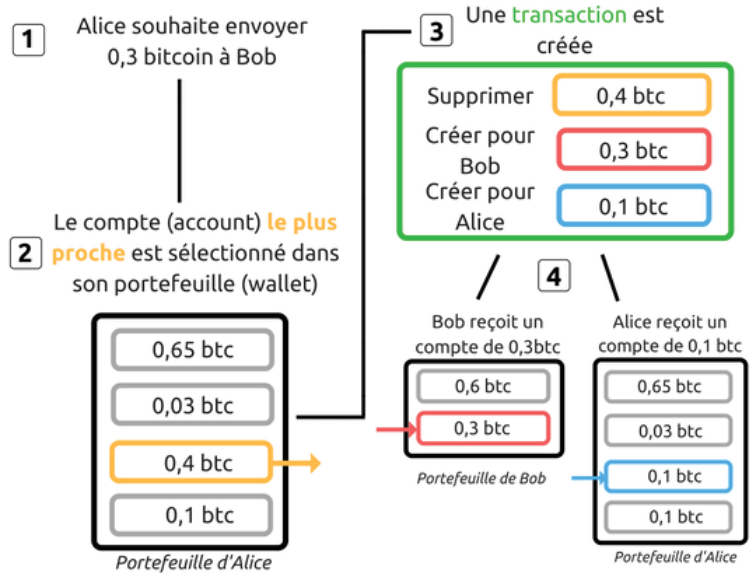
[1] *Cf.* https://journalducoin.com/blockchain/ethereum-la-blockchain-aux-pieds-dargile/

3. L'absence de recours au protocole « UTXO »

Pour s'assurer collectivement de l'équilibre des entrées et des sorties, sans recourir à un tiers de confiance, le protocole du bitcoin prévoit un système particulier, qui a été repris par d'autres cryptomonnaies.

Chaque transaction, visible car inscrite dans un bloc, inclut ainsi la **suppression d'une « sortie » (*output*) appartenant à l'émetteur, et la création de trois autres**. L'une est à destination du récepteur, une autre à destination du mineur (frais de transaction), une troisième, éventuelle, correspond au change et est renvoyée à l'émetteur, c'est elle qui est appelée *Unspent Transaction Output* (UTXO). Elles font partie des **innovations introduites par Bitcoin qu'Ethereum a choisi d'écarter**.

Décomposition d'une transaction en bitcoin



Source : OPECST

Un des principaux arguments en faveur de l'approche UTXO est la **montée en charge** ou scalabilité. Étant donné que les soldes sont stockés comme un ensemble de transactions sortantes, l'ordre dans lequel elles sont effectuées n'a pas d'importance. Ce système permet donc d'éviter qu'un tiers de confiance ne soit sollicité dans le but de tenir à jour les comptes des utilisateurs.

Cette technique **utilisée** d'abord **par le bitcoin** puis par d'autres cryptomonnaies n'a **pas été retenue pour l'ether**, car elle présente certaines limites. Un tel système suppose en effet la création de plus en plus d'UTXO, qui ont chacune une valeur de plus en plus faible, ce qui nécessite un **espace de stockage croissant** et crée peu à peu des « poussières de comptes », qui peuvent finir par être lourds pour le réseau. Il explique notamment aussi les

disparités de capacité entre Bitcoin et des réseaux de paiement traditionnels (200 000 transactions quotidiennes en bitcoins contre 150 millions pour Visa par exemple).

D'autres cryptomonnaies, en plus de l'ether, ont donc plutôt choisi de fonctionner avec un **équilibrage des comptes et soldes** comparable à celui d'un système bancaire classique.

B. LES AUTRES CRYPTOMONNAIES

1. Plus de 1 600 cryptomonnaies distinctes en juin 2018

Toutes les *blockchains* des cryptomonnaies sont plus ou moins des **avatars de celle du bitcoin**, comme l'explique Stéphane Loignon. Selon ce dernier, elles en reprennent « *les grands principes mais changent tel ou tel aspect, pour compenser ce que leurs créateurs estiment être un défaut de leur ancêtre. Pour accélérer l'enregistrement des transactions et diminuer la consommation d'énergie du réseau, certaines modifient leur mécanisme de consensus. Pour élargir les usages possibles, d'autres, comme Ethereum, adaptent le langage informatique pour rendre possible l'inscription de programmes élaborés (*smart contracts*). Pour garantir plus de confidentialité à leurs clients, quelques-unes (comme celles sur lesquelles les banques travaillent par exemple) renoncent au caractère public de la blockchain et optent pour un réseau fermé : on les appelle alors des blockchains privées (ou de consortium). Enfin, pour gérer les éventuelles erreurs et éviter qu'elles soient fixées pour de bon dans la chaîne de blocs, l'entreprise Accenture a même poussé l'inventivité jusqu'à concevoir ce qui pour beaucoup apparaît comme une contradiction dans les termes : une blockchain révisable, qu'une autorité centrale a la possibilité d'amender après coup* ».

Le site *coinmarketcap.com*, dont est issu le tableau ci-après, recense à ce jour **plus de 1 600 cryptomonnaies distinctes**, plus d'une dizaine faisant leur apparition chaque semaine.

Classement des principales cryptomonnaies en termes de capitalisation au 8 juin 2018

#	Nom	Symbole	Capitalisation totale	Prix unitaire	Nombre d'unités en circulation
1	Bitcoin	BTC	$129 531 586 691	$7 582,89	17 082 087
2	Ethereum	ETH	$59 782 737 373	$598,16	99 944 559
3	Ripple	XRP	$26 080 082 651	$0,664557	39 244 312 603 *
4	Bitcoin Cash	BCH	$18 918 942 413	$1 101,72	17 172 188
5	EOS	EOS	$12 385 861 361	$13,82	896 149 492 *
6	Litecoin	LTC	$6 771 451 402	$119,03	56 890 523
7	Stellar	XLM	$5 336 386 812	$0,286857	18 602 951 338 *
8	Cardano	ADA	$5 267 888 119	$0,203181	25 927 070 538 *
9	IOTA	MIOTA	$4 663 078 979	$1,68	2 779 530 283 *
10	TRON	TRX	$3 759 371 827	$0,057178	65 748 111 645 *

Source : coinmarketcap.com

À ce dynamisme notable s'ajoute la **grande volatilité des cours** et des **positions relatives**, en-dehors du bitcoin qui conserve la première place en termes de capitalisation totale (en baisse toutefois : elle est passée de 95 % en 2013 à moins de 40 % aujourd'hui). L'ether fortifie quant à lui peu à peu sa deuxième position. La position dominante du bitcoin a failli être contestée par l'ether à l'été 2017, mais elle s'est confirmée ensuite.

Il est essentiel de **ne pas s'arrêter à ce simple classement**, non seulement en raison de sa forte variabilité, mais aussi tant certains actifs qu'il compare sont de natures distinctes.

Toutefois, le code source des *blockchains* Bitcoin ou Ethereum étant librement accessible, certaines de ces cryptomonnaies n'en sont à l'inverse que des dérivés plus ou moins proches ou plus ou moins éloignées. Pour Ricardo Perez-Marco, directeur de recherche au CNRS, comme pour Pierre Porthaux, entrepreneur, la grande majorité des cryptomonnaies actuelles sont vouées à disparaître rapidement.

La composition du marché des cryptomonnaies depuis 2013

Source : coinmarketcap.com

2. Quelques exemples

Ripple fait partie des cryptomonnaies sensiblement différentes de Bitcoin et d'Ethereum. Elle utilise en effet un réseau partiellement centralisé afin de permettre des transactions financières très rapides. Sa forte capitalisation serait directement liée à son activité auprès de grands organismes bancaires, qui relève d'une *blockchain* de consortium. Beaucoup d'observateurs refusent ainsi de considérer Ripple comme une véritable *blockchain*, « *c'est la monnaie la plus détestée de tout l'écosystème* », selon Jean Zundel.

Stellar est un réseau destiné à échanger des monnaies classiques entre elles, ou avec d'autres cryptomonnaies, par le biais d'une monnaie appelée lumen. Elle est très proche de Ripple, dont elle partage les mêmes fondateurs et a **besoin d'institutions existantes,** qu'elle appelle « ancres » (*anchors*) afin de garantir les dépôts et les retraits dans une devise spécifique. Cela fait de Stellar, à l'instar de Ripple, un système très éloigné de l'idéal originel des premières *blockchains* publiques.

Avec l'augmentation des transactions en bitcoins, le projet initial, Bitcoin Core, a fait l'objet de nombreuses critiques. Un certain nombre de développeurs souhaitaient faciliter sa montée en puissance en élargissant la taille des blocs afin d'y faire transiter un plus grand nombre de transactions. Ils proposèrent à l'adoption du réseau une version modifiée du code source du bitcoin le 1er août 2017. Celle-ci fut loin de faire l'unanimité, mais certains nœuds l'adoptèrent quand même. Cette « *hard fork* » fut à l'origine de **Bitcoin Cash**, une nouvelle cryptomonnaie partageant le même historique que Bitcoin Core, mais au fonctionnement désormais totalement indépendant. De la même manière apparut **Bitcoin Gold** en octobre 2017, suite à l'échec de l'adoption d'une autre modification du code.

D'autres cryptomonnaies empruntent au code source du bitcoin sans toutefois chercher à convaincre l'ensemble du réseau de l'adopter avec eux. Ce fut le cas de **Litecoin**, qui permet une création de blocs plus rapide et qui se donnait pour but d'utiliser du matériel informatique standard pour le minage, permettant à chacun d'y participer (cet objectif n'a pu être atteint). Cette *blockchain* a elle-même connu son propre *fork* le 18 février 2018 avec l'adoption de **Litecoin Cash**. **DASH**, créé en 2012, est un autre dérivé du code source du bitcoin, initialement appelé darkcoin, qui permet notamment des transactions immédiates (*InstantSend*) ou anonymes (*PrivateSend*).

D'autres monnaies sont des dérivés d'Ethereum, comme **Ethereum Classic**, créée par les nœuds ayant refusé la *hard fork* TheDAO. On trouve aussi **EOS**, créée par d'anciens développeurs de la *blockchain* de l'éther, qui vise à concurrencer le premier dans le domaine des *smart contracts*, c'est-à-dire des programmes automatisés sur la *blockchain*.

Cardano est une autre solution proche d'Ethereum, mais qui se distingue de la plupart des autres cryptomonnaies par son développement par le groupe IOHK, composé d'universitaires. La documentation de Cardano est publique et a fait l'objet d'articles publiés dans des revues à comité de lecture. Son algorithme de consensus, dénommé Ourobouros, est prouvé mathématiquement et fonctionne avec la preuve d'enjeu.

Zcash, dont le protocole est appelé *zerocash*, et **Monero**, sont deux monnaies dont l'objectif est de garantir la confidentialité des transactions grâce à des méthodes cryptographiques complexes. Leur fonctionnement sera évoqué dans la deuxième partie de ce rapport, en lien avec les problématiques de protection des données personnelles.

Enfin, d'autres cryptomonnaies sont à observer avec une particulière circonspection, comme **Tron**, dont plusieurs parties du livre blanc originel sont simplement des plagiats de plusieurs autres projets, ou **Tether**, une escroquerie très probable créée par les propriétaires d'une grande plateforme d'échange de bitcoins.

Le projet **Iota** veut utiliser un protocole sensiblement différent des *blockchains* classiques, mais n'échappe pas lui aussi à une très sévère critique de la plupart des experts.

Ledger n'est pas une cryptomonnaie mais une société française qui mérite d'être mentionnée car elle commercialise des portefeuilles de cryptomonnaies sécurisés ou *wallets*, sous une forme physique (*hardware*) ou dématérialisée. Son potentiel est de premier ordre et elle serait, pour certains journalistes, une future « licorne »[1].

Le projet français **Neurochain** est lui aussi sensiblement différent des *blockchains* originelles en faisant appel à l'intelligence artificielle et, en particulier, à l'apprentissage automatique (*machine learning*). Les nœuds du réseau y supportent des « bots », c'est-à-dire des systèmes communiquant entre eux pour former une intelligence artificielle collective capable de valider des blocs de manière sécurisée, décentralisée et transparente, sans recours à la preuve de travail[2].

---

[1] *L'expression inventée par Aileen Lee en 2013 renvoie à une start-up valorisée ou potentiellement valorisée plus d'un milliard de dollars, cf.* http://fortune.com/2015/01/22/the-age-of-unicorns/

[2] *La note de présentation technologique («* white paper *») du projet permet d'en savoir plus, cf.* https://developers.neurochaintech.io/documentation/technical-white-paper/

VI. LA DISTINCTION ENTRE *BLOCKCHAIN*S OUVERTES OU PUBLIQUES ET *BLOCKCHAIN*S FERMEES OU PRIVEES

A. ÉVITER UNE CONFUSION FREQUENTE

La distinction *blockchain*s publiques/*blockchain*s privées **ne repose pas sur une distinction entre *blockchain*s de personnes publiques** (États, collectivités…) **et *blockchain*s de personnes privées** (entreprises, ONG…), **mais sur le caractère ouvert ou fermé de la *blockchain***, les protocoles de chaînes de blocs pouvant être distingués selon qu'ils sont ouverts à l'écriture et à la lecture sans restriction ou que l'une ou l'autre de ces opérations est soumise à l'acceptation d'un tiers. Cette distinction peut aussi résulter de l'utilisation ou non d'une cryptomonnaie comme méthode d'incitation. On parlera alors de *blockchain*s ouvertes (*permissionless*) ou fermées (*permissioned*) ou encore de *blockchains* publiques ou privées.

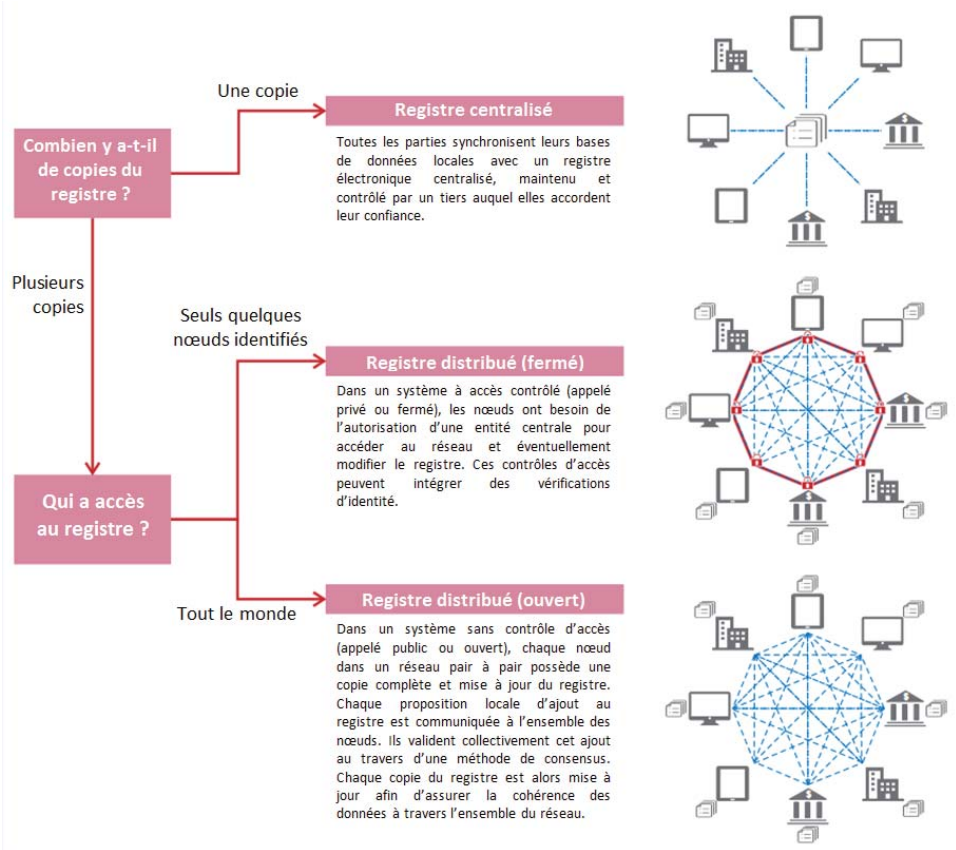
Les protocoles de *blockchain*s **sans restriction d'accès** sont **les plus connus**. Ils soutiennent le bitcoin ou l'ether. Comme il a été vu, n'importe qui peut en devenir un nœud, et ces protocoles nécessitent une méthode de consensus.

B. LES BLOCKCHAINS PRIVEES SONT-ELLES DE « VRAIES » BLOCKCHAINS ?

Il existe aussi un grand nombre **de protocoles à restriction d'accès**, pour certains particulièrement aboutis et déjà opérationnels. Parmi ces derniers, les *blockchains* « de consortium » résultent du regroupement de plusieurs organisations indépendantes, voire concurrentes, utilisant la *blockchain* pour archiver dans un registre décentralisé des transactions sécurisées, ou échanger des actes certifiés, sans avoir à faire intervenir un tiers de confiance. D'autres protocoles sont utilisés au sein d'une même organisation, pour simplifier et automatiser des échanges et des certifications.

Dans une *blockchain* privée, **une autorité régulatrice** valide l'introduction de nouveaux membres, et accorde les droits en écriture et en lecture. Cette autorité peut être seule aux commandes ou gouvernée collégialement par les différents participants. À la différence d'une *blockchain* publique, les *blockchains* privées peuvent exiger une majorité renforcée. De même, il suffit de trois participants pour faire fonctionner une *blockchain* privée, tandis que les *blockchains* publiques doivent en compter plusieurs milliers pour se développer.

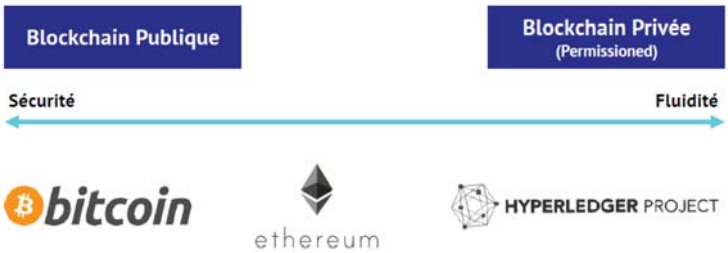
Différents types de registres selon leur caractère centralisé ou distribué et leur caractère ouvert ou fermé



Source : OPECST d'après le chapitre « Cryptocurrencies : looking beyond the hype » du rapport annuel 2018 de la Banque des règlements internationaux, et la note de la Banque mondiale « Distributed ledger technology and blockchain » par H.Natarajan, S.Krause and H.Gradstein, 2017

Deux projets majeurs de *blockchains* privées méritent d'être évoqués. Le premier, **Hyperledger**, a été lancé il y a deux ans par la fondation Linux, et réunit aujourd'hui plus de 85 membres, dont Accenture, Airbus, Fujitsu, JP Morgan, Intel ou encore IBM. Le second est le **consortium interbancaire R 3**, qui se veut un registre distribué pour les services financiers. Il compte en son sein, entre autres, les établissements suivants : Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J. P. Morgan, Royal Bank of Scotland, State Street, UBS...

Exemples de *blockchains* selon leur caractère ouvert ou fermé



Source : Présentation de Simon Polrot

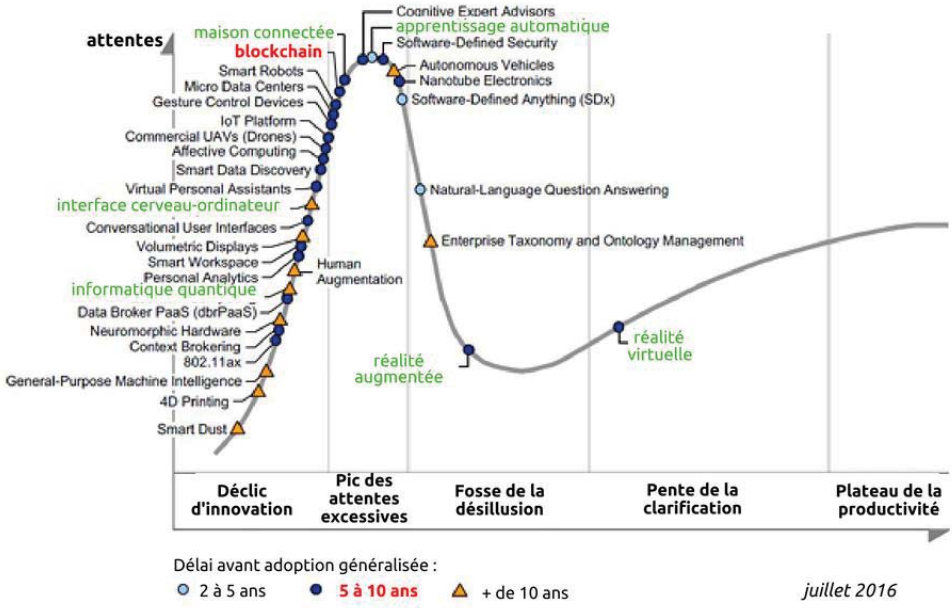
Il est possible de rapprocher les *blockchains* publiques d'internet et les *blockchains* privées d'intranets, dans la mesure où ces deux catégories sont différentes dans leurs modalités de fonctionnement tout en présentant certaines similitudes.

Un débat existe pour qualifier les *blockchains* privées de « vraies » ou de « fausses » *blockchains*, sachant que créer un produit recourant à ces technologies est aussi un **enjeu de marketing**. Le recours de certaines applications aux *blockchains* ne semble pas toujours justifié, les fonctionnalités offertes par les bases de données partagées et sécurisées existantes apparaissant en effet suffisantes à leur réalisation.

Un regard plus distancié paraît nécessaire, en raison des **effets de mode propres aux écosystèmes entrepreneuriaux**. Ces effets de mode, visibles dans le recours à certains concepts, tels que les technologies disruptives, l'intelligence artificielle, les données massives (*big data*), le *cloud*, l'internet des objets (IoT pour *internet of things*) ou, encore, la *blockchain,* sont parfois le reflet de stratégies marketing séduisantes, mais sans toujours s'accompagner d'innovations aussi majeures que celles annoncées.

Pour certains observateurs, **l'effet de mode autour de la *blockchain* serait aujourd'hui à un sommet** et l'on serait donc **proche d'une sortie** de cette position extrême.

L'effet de mode autour de la *blockchain*



Source : OPECST d'après Gartner.com[1].

La question de savoir **comment les différentes *blockchains* pourront s'intégrer et/ou devenir interopérables** n'est pas encore tranchée. Une étude du réseau interbancaire *European Financial Management Association* (EFMA) et du cabinet Deloitte assure que pour 53 % des institutions financières interrogées, c'est la « *blockchain privée détenue par un consortium* » qui permettra l'adoption à grande échelle de cette technologie (seuls 11 % misent sur la *blockchain* publique)[2]. Pour certains, comme Quentin de Beauchesne, « *les blockchains privées n'ont pas vraiment d'avenir (…) l'avenir appartient aux plateformes privées bâties au-dessus de blockchains publiques, des « sur-couches », comme ce que nous proposons chez Ledgys* ».

[1] *Cf.* https://www.gartner.com/newsroom/id/3412017

[2] *Cf. Deloitte, EFMA, "*Out of the Blocks"*, 2016.*

VII. LES TECHNOLOGIES DE REGISTRES DISTRIBUES ALTERNATIVES AUX *BLOCKCHAINS*

A. DES LEDGERS FONDES SUR DES « GRAPHES ORIENTES ACYCLIQUES » (DIRECTED ACYCLIC GRAPHS OU DAG)

1. Des projets en développement

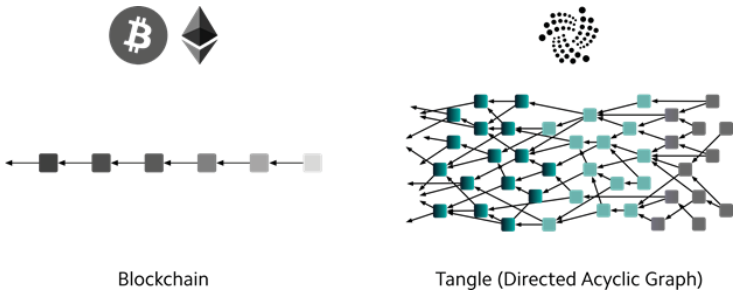
Plusieurs technologies de **registres distribués** (*ledgers*), alternatives aux *blockchains*, sont en développement. Tout en présentant les mêmes intérêts en termes de décentralisation, elles sont annoncées comme **plus rentables** (pas de preuve de travail), **plus rapides, plus efficaces**, **moins exposées à une prise en main du réseau** (pas de mineurs) et, surtout, **moins chères** (pas de frais).

Ces technologies permettraient de créer des blocs et d'en communiquer la trace sur un réseau pair à pair, en suivant le principe des « graphes orientés acycliques » (*Directed Acyclic Graphs* ou DAG). Elles utilisent la technique du « *gossip about gossip* » : il s'agit pour un nœud d'attacher à un ensemble d'informations créé (un *gossip*), les hashs des deux derniers utilisateurs ayant eu une interaction avec lui.

2. Des registres distribués qui forment des réseaux maillés

Plutôt qu'une chaîne, l'ensemble des transactions prend alors la forme d'un **réseau maillé**, d'un graphe de hashs. Sur ce graphe, il est possible de déterminer quel chemin a été « choisi » par un maximum de nœuds, et donc d'atteindre un consensus, cette opération allant extrêmement vite. On peut parler de « vote virtuel » car le « vote » de chaque nœud est anticipé.

Structure schématique d'un registre en *DAG* par rapport à une *blockchain*



Source : site internet du projet IOTA, iota.org

B. DES TECHNOLOGIES ENCORE PEU MURES

1. Un problème de fiabilité

Il reste **difficile de s'assurer de la fiabilité de ces réseaux**, singulièrement plus complexes que les protocoles de *blockchain*, en particulier pour un déploiement dans un système ouvert (*permissionless*). Ils semblent moins aptes à se prémunir contre les différentes formes d'attaques, en particulier les attaques *Sybil*.

Ainsi, la technologie de DAG la plus connue, *Tangle*, de l'entreprise *IOTA* qui veut étendre les principes des *blockchains* à l'internet des objets (IOT), reçoit de **très fortes critiques** de la part des observateurs. Elle est qualifiée tant par Jean Zundel, spécialiste d'Ethereum, que par Pierre Porthaux, entrepreneur, « *d'arnaque* ».

Moins connu, l'algorithme *HashGraph*, développé par une société texane sur la plateforme *Swirlds*, n'en semble pas moins **voué à l'échec**. En effet, la consultation de son code est soumise à une licence d'utilisation, ce qui l'invalide dans l'écosystème classique des registres distribués au sein duquel les logiciels ouverts (*open source*), librement accessibles donc, sont la norme. Cette modalité juridique de déploiement n'est pas de nature à aider à son adoption par les acteurs.

2. Une alternative encore très hypothétique

Pour ces raisons, ces deux projets évoqués durant les auditions ont reçu **très peu de soutien** et la **perspective d'un remplacement** des *blockchains* par des solutions utilisant des graphes acycliques distribués **semble encore très hypothétique**.

Jean Zundel a toutefois souligné qu'un projet peu connu, Byteball, était à ce stade un *ledger* alternatif plus fonctionnel et plus complet, mais qui doit lui aussi faire ses preuves.

DEUXIEME PARTIE :

LES ENJEUX DES *BLOCKCHAINS*

I. LES DEFIS DE LA MONTEE EN CHARGE (« SCALABILITE ») ET DE LA SECURITE

A. REPONDRE AU DEFI DU NOMBRE DE TRANSACTIONS

1. Une question décisive

La **capacité à faire face à une augmentation du nombre de transactions** constitue l'un des principaux défis pour les *blockchain*s, à commencer par celle du bitcoin. Cette dernière ne permettait jusqu'en 2017 la validation que de quatre transactions par seconde en moyenne (autour de 20 en 2018). Ce défi de la montée en charge (scalabilité) reste entier. Il a conduit à accélérer la naissance de plus de 1 600 cryptomonnaies à ce jour, souvent dites alternatives (« *altcoins* »).

Ce défi s'est également traduit par la recherche de **pistes de réponse technologiques**.

2. Des solutions encore en développement

Il a ainsi mené à des **innovations encore peu matures d'un point de vue technologique**, comme la parallélisation de *blockchain*s collatérales, aux fonctions différentes et complémentaires (« *sidechains* » pour le bitcoin, « *sharding* » ou « *plasma chains* » sur Ethereum), le recours à des bases de données liées à la *blockchain* (« *side databases* »), ou encore la création d'une nouvelle couche de protocole allégé et rapide « au-dessus » de la *blockchain* mais bénéficiant de sa sécurité (« *lightning networks* » pour le bitcoin, « *state channels* » sur Ethereum).

Pour Laurent Benichou, cadre chez Axa France, « *l'idée est de désengorger la blockchain du bitcoin, en mettant des transactions dans des blockchains satellites, qui ont un point de contact avec la blockchain principale Bitcoin. Imaginons que je vende et achète des actions toutes les secondes, elles seront toutes répertoriées dans une blockchain satellite et j'inscrirai seulement à la fin de la journée le montant total des achats et des ventes dans la blockchain principale* ». Selon Claire Balva, la cofondatrice de Blockchain France, il serait « *tout à fait possible qu'il y ait une, deux ou trois blockchains publiques dominantes, accompagnées d'une foison de blockchains privées ou de sidechains, qui fonctionneraient un peu comme des intranets* ».

Les UTXO, présentés précédemment et utilisés notamment par le bitcoin mais pas par l'ether, ont pour principal avantage de permettre une plus grande montée en charge car ils permettent à un même compte de faire plusieurs transactions de manière simultanée, sans qu'il soit besoin d'attendre qu'une transaction soit effectuée pour modifier le solde d'un compte et autoriser ou non la production d'une nouvelle dépense.

B. REPONDRE AU DEFI DES RISQUES D'ATTAQUES

La **sécurité** est probablement la caractéristique des *blockchains* la plus mise en avant. Effectivement, il est plus ardu de pirater un registre distribué entre plusieurs milliers de « nœuds » disséminés à travers le monde, que présent sur un unique serveur centralisé. Si la longévité de la *blockchain* du bitcoin semble une garantie de l'intégrité de ses transactions, **elle n'est pas, en réalité, exempte de failles** et **a déjà été attaquée**. Les autres protocoles, en particulier ceux qui développent des applications complexes, sont au moins autant exposés à des attaques, en proportion de leur valeur financière.

1. Attaques contre les interfaces

Plus une *blockchain* possède un réseau étendu et dispersé, plus il est difficile de modifier son code ou de créer une transaction frauduleuse. Ainsi, beaucoup de piratages recensés (vols massifs de cryptomonnaies, en particulier) ne portaient pas sur le protocole lui-même mais sur des interfaces avec celui-ci, tels que des sites internet de change. De telles attaques consistent simplement à subtiliser les clés privées confiées par des utilisateurs à ces sites et à les utiliser afin de transférer les sommes en cryptomonnaies auxquelles elles correspondent vers un autre compte.

La **disparition de 850 000 bitcoins en février 2014** (l'équivalent de 660 millions de dollars au cours du 10 décembre 2016) de la plateforme japonaise MtGox, alors l'une des principales places d'échange de bitcoins au monde, témoigne de cette vulnérabilité. Plus récemment, en août 2016, 120 000 bitcoins (l'équivalent de 93 millions de dollars au cours du 10 décembre 2016) ont été subtilisés à Bitfinex, l'une des principales « bourses » de bitcoin. Selon une estimation de l'agence Reuters, un tiers des plateformes d'échange auraient ainsi été hackées depuis 2009[1].

2. Attaques contre les applications et le cas de TheDAO

Plusieurs *blockchains* cherchent à dépasser le simple usage transactionnel pour proposer des applications plus développées, qui prennent la forme de programmes informatiques inscrits dans la chaîne de blocs, des *smart contracts*. Ces perspectives nouvelles ont cependant une contrepartie en termes de sécurité, **ces programmes ajoutant de la complexité dans le protocole** et, par voie de conséquence, de **potentielles failles exploitables par des attaquants**. Pour le professeur Gérard Memmi, en raison de l'immuabilité du code inscrit dans la *blockchain*, les erreurs de programmation dans les *smart contracts* sont particulièrement gênantes.

---

[1] *Gertrude Chavez-Dreyfuss, « Cyber Threat Grows for Bitcoin Exchanges », Reuters, 29 août 2016.*

Ces risques sont d'autant plus élevés que les langages de script mis sur pied pour Bitcoin ou Ethereum l'ont été dans des délais bien plus restreints que ceux qui prévalent normalement, sous l'effet d'un besoin rapide de nouvelles solutions. Selon Vincent Danos, chercheur en informatique, la solidité de ces langages de programmation ne peut pas être vérifiée par une simple lecture mais demande à être testée de manière itérative avec des outils complexes conçus à cette fin. Il en résulte, selon Gérard Memmi, qu'on ne peut pas dire aujourd'hui que les *smart contracts* sont techniquement au point.

Le **cas du piratage de l'application TheDAO** (T*he Decentralized Autonomous Organisation)* sur Ethereum est probablement le plus emblématique à ce titre. Le très ambitieux projet TheDAO cherchait en effet à repousser les limites offertes par les *smarts contracts* en recréant le fonctionnement complet d'une organisation en permettant par exemple le vote, l'élection, la certification, la rémunération… Chaque utilisateur de TheDAO devait ainsi pouvoir participer au fonctionnement d'une organisation sans autorité centrale de contrôle, ayant pour but de financer des projets en échange de revenus. Il s'agissait d'un système à mi-chemin entre actionnariat et financement par la foule (*crowdfunding)*. Cent-cinquante millions d'euros furent collectés sous forme d'ethers pour une opération qui n'en nécessitait que quelques centaines de milliers.

Le 17 juin 2016, un *hacker a* utilisé une vulnérabilité dans une fonction du contrat pour détourner un tiers de la somme collectée en ethers, ce qui correspondait alors à près de 5 % de la totalité des ethers en circulation. Faisant face à un vol d'une telle ampleur, mais alors que le protocole en lui-même n'était pas mis en danger, les développeurs décident de proposer au réseau d'adopter une mise à jour afin de revenir à un état antérieur du registre, tout en conservant l'ensemble des transactions échangées sur la *blockchain* depuis l'accident. Cette proposition ayant été massivement acceptée, elle a donné lieu à un *hard fork*.

3. Attaques utilisant le procotole

Le protocole d'une *blockchain* « *permissionless* », c'est-à-dire ouverte à tous, ne prévoit, par définition, aucune gouvernance, donc aucun moyen de contrôle ou de sanction. Tant qu'il respecte le fonctionnement du protocole, un utilisateur malveillant peut donc réaliser des actions frauduleuses sans encourir le risque d'une pénalité. Dans un contexte de preuve de travail, l'attaque la plus évidente est celle des 51 % : il s'agit pour un mineur de réunir plus de 50 % de la puissance de calcul à un instant donné, et ainsi de pouvoir valider des blocs plus rapidement que l'ensemble des autres utilisateurs. Cela lui permet alors d'effectuer des double dépenses, c'est-à-dire de réaliser plusieurs transactions avec la même unité de cryptomonnaie. Une autre technique, appelée *eclipse attack*, consiste à présenter à un nœud donné une fausse version du registre, de sorte que celui-ci ne puisse pas se prémunir d'une double transaction de la part de l'assaillant. En pratique, il s'agit pour l'assaillant de **prendre le contrôle de tous les nœuds connectés à un utilisateur donné**.

Il est assez simple d'envisager le coût d'une **attaque 51 %** dans un système utilisant la preuve de travail, puisqu'elle est égale au coût lié à la puissance de calcul de l'ensemble du réseau. Ainsi, la *blockchain Bitcoin Gold*, dont la capitalisation dépasse les 500 millions de dollars, a subi une telle attaque le 24 mai 2018.

De ce point de vue, la *blockchain* du bitcoin semble particulièrement sûre : au vu du nombre de mineurs et de la quantité d'argent en jeu pour récompenser leur minage, aucune double dépense ne semble suffisamment rentable pour compenser les moyens à investir dans une attaque 51 %. Cette sécurité repose sur l'hypothèse d'une rationalité de l'attaquant, celui-ci ne pouvant pas envisager une opération qui lui coûterait plus qu'elle ne lui rapporterait. Il

est cependant possible qu'un attaquant fortement doté en moyens (comme un gouvernement ou une multinationale) souhaite simplement s'attaquer au réseau pour créer un bouleversement économique à l'échelle mondiale à des fins politiques, c'est ce qu'on appelle une attaque *Goldfinger*.

Il est à noter que les *blockchains* fermées ou *permissionned*, ne sont pas susceptibles de subir une attaque 51 % car les membres du réseau sont connus et un contrôle est donc possible. Elles ne sont cependant pas à l'abri d'un *bug* dans leur code source.

4. Attaques contre le protocole lui même

Enfin, bien que les protocoles soient en accès libre et que les communautés qui les entourent s'assurent de leur sécurité, une **faille dans leur code même n'est pas inenvisageable** ou pourrait apparaître avec les progrès de l'informatique. Ainsi, les primitives cryptographiques soutenant les algorithmes de signature ECDSA ont une durée de vie limitée à long terme, en particulier dans le cas hypothétique du développement de l'ordinateur quantique, dont la faisabilité reste toutefois sujette à caution. Une telle évolution n'est pas une menace pour les fonctions de hachage, mais leur espérance de vie reste tout de même limitée, entre 20 et 100 ans pour SHA-256, selon les experts.

En outre, même les plus anciens protocoles ne sont pas à l'abri d'une faille. Ainsi, **le bitcoin a été attaqué avec succès le 15 août 2010** à l'occasion de ce que l'on a appelé le *value overflow incident* et la découverte que le bloc 74638 contenait une transaction créant 184 467 440 407 bitcoins (soit environ 184 milliards de bitcoins) pour 3 adresses différentes. À l'époque cependant, le bitcoin était loin d'avoir sa valeur actuelle. Lors de cette attaque, deux adresses ont reçu 92,2 milliards de bitcoins chacune. L'erreur provient de ce que le code utilisé pour vérifier les transactions avant de les inclure dans un bloc ne prenait pas en compte des valeurs aussi grandes, ce qui explique le nom de « bug de dépassement de capacité ».

Une nouvelle version du client (programme gérant un nœud) a été publiée moins de 5 heures après la découverte du bug. Cette correction rejette toute transaction de plus de 21 millions de bitcoins. Cependant, de nombreux nœuds non corrigés ont continué à construire la « mauvaise » *blockchain* pendant plusieurs heures. La « bonne » *blockchain* finit par s'imposer neuf heures après le début de l'incident, au bloc 74691, ce qui provoqua l'annulation des transactions frauduleuses, mais aussi d'autres transactions qui ne l'étaient pas.

II. D'AUTRES APPLICATIONS QUE LES CRYPTOMONNAIES POUR LA *BLOCKCHAIN* ?

Le rôle de la *blockchain* en tant que **technologie sous-jacente des nombreuses cryptomonnaies** est aujourd'hui dominant. Cependant, ses protocoles se **déclinent dans de nombreux secteurs** et pourront donner naissance à des applications nouvelles variées, dépassant le cadre strict de la finance. Pour l'entrepreneur Dom Steil, « *de même qu'internet a été la base de bien d'autres applications que le courrier électronique, la blockchain sera la base de bien d'autres applications qu'un réseau de paiement* ».

Selon les personnes auditionnées par vos rapporteurs, l'idée de Jean-Claude Trichet selon laquelle on peut imaginer des utilisations de la *blockchain* tout en rejetant les cryptomonnaies et, en particulier le bitcoin, serait cependant en grande partie un mythe : **d'autres usages sont possibles mais ils ne pourront que difficilement se déployer sans les cryptomonnaies**. Selon Jean-Claude Trichet dans une interview au journal *Le Monde* en 2016, la *blockchain* serait en effet « *une invention géniale, parce qu'elle repose sur une*

décentralisation complète de l'enregistrement des transactions. Au lieu d'avoir un système central qui enregistre et qui contrôle tout, on est en présence d'une technologie impressionnante testée sur beaucoup d'applications qui n'ont rien à voir avec le bitcoin ». Néanmoins affirmer que les applications possibles de la *blockchain* n'ont rien à voir avec les cryptomonnaies est imprécis : **aujourd'hui les *blockchains* publiques ne se développent pas sans l'émission d'une cryptomonnaie**[1].

Cette analyse contraste avec celle de Christine Lagarde, qui expliquait le 13 mars 2017, dans un article de la revue du FMI « *que la valeur de Bitcoin augmente ou qu'elle diminue, tout le monde se pose la même question : quel est exactement le potentiel des crypto-assets ? La technologie derrière ces actifs, y compris la blockchain, constitue une avancée passionnante qui pourrait aider à révolutionner d'autres domaines que la finance […] Il ne serait pas judicieux de rejeter les crypto-assets […] Nous pouvons exploiter le potentiel des crypto-actifs tout en veillant à ce qu'ils ne deviennent jamais un refuge pour les activités illégales ou une source de vulnérabilité financière* ». Pour elle, les applications autres que les cryptomonnaies pour la *blockchain* sont donc souhaitables et passeront par un développement de ces actifs financiers. Plus récemment, la directrice générale du FMI s'est voulue rassurante, à l'occasion d'une conférence organisée par la Banque d'Angleterre, en septembre 2017, par rapport aux défauts éventuels des cryptomonnaies : « *les monnaies virtuelles […] produisent leur propre unité de compte et leur propre système de paiement. Ces systèmes permettent des transactions de pair à pair, sans chambre de compensation, sans banque centrale. À l'heure actuelle les monnaies virtuelles comme bitcoin ne représentent pas encore de menace pour l'ordre existant des monnaies fiduciaires et des banques centrales. Pourquoi ? Parce qu'elles sont trop volatiles, trop risquées, trop énergivores, parce que les technologies sous-jacentes ne sont pas suffisamment scalables, que beaucoup d'entre elles sont trop opaques pour les régulateurs et que certaines ont été piratées. Mais beaucoup de ces défauts ne sont que des défis technologiques qui pourraient être surmontés avec le temps ».*

En plus de la fonctionnalité puissante offerte en matière d'échanges financiers grâce aux cryptomonnaies, Stéphane Loignon explique que la *blockchain* offre deux autres usages majeurs : elle permet « *d'enregistrer de l'information de manière immuable, des actes administratifs, des titres de propriété ou encore des diplômes peuvent y être inscrits sans pouvoir être modifiés par la suite, ce qui offre une garantie d'authenticité que fournissaient jusqu'ici les notaires* » et elle donne la « *possibilité d'héberger des programmes qui automatiseront des communications et des transactions entre des personnes et entre les milliards d'objets connectés du monde entier* » à travers les *smart contracts*.

---

[1] *Le rapport de France Stratégie* « Les Enjeux des blockchains »*, partage cette analyse : «* on a voulu instaurer une sorte de cordon sanitaire entre les cryptomonnaies, considérées avec une certaine suspicion, et la blockchain, considérée comme très prometteuse. Utile dans un premier temps pour laisser se déployer l'innovation malgré les problèmes de fraude que posent certains usages des cryptomonnaies, cette séparation commence à poser problème. De fait, les protocoles de consensus qui sont au cœur des blockchains publiques reposent tous sur des mécanismes d'incitation économique qui requièrent l'émission d'un actif numérique. Cet actif permet d'inciter les différents acteurs à participer à la sécurisation du réseau – le protocole attribuant automatiquement un certain nombre de « jetons » aux validateurs des nouveaux blocs. Ce fonctionnement fait des actifs numériques une des pierres angulaires des blockchains publiques. Pour séparer le bon grain de l'ivraie et bénéficier des seuls effets souhaités des blockchains, il ne suffira donc pas d'essayer d'interdire ou de contrôler le bitcoin *».*

Ces trois fonctionnalités, parfois combinées, pourraient conduire à d'importantes évolutions économiques et sociales. Par exemple, la possibilité de faire des transactions en ligne sans intermédiaire a des impacts sur l'ensemble du secteur financier. De même, la *blockchain* bouleverse l'économie numérique : un site commercial utilisé pour acheter un bien ou un service pourrait être réformé en version pair à pair.

La *blockchain* Ethereum offre une infrastructure adaptée à des outils tels que des codes informatiques qui peuvent s'exécuter après avoir été écrits dans une *blockchain*, qu'il s'agisse de *smart contracts*, d'applications décentralisées dites « Dapps » ou d'organisations autonomes décentralisées appelées « DAO » (*Decentralized Autonomous Organizations*), organisations collectives dont les règles de fonctionnement et les procédures sont inscrites sur la *blockchain*.

Les Dapps sont, quant à elles, des applications décentralisées, en réalité distribuées, qui fonctionnent grâce à des programmes inscrits sur la *blockchain*. Leur utilisation nécessite toutefois l'intervention d'un tiers. 819 projets sont ainsi recensés sur le site « *state of the Dapps* » (état des Dapps) et peuvent concerner les marchés prédictifs, l'assurance, les places de marché décentralisées, ou encore les jeux vidéo.

A. DES SERVICES D'ATTESTATION ET DE CERTIFICATION GRACE AUX BLOCKCHAINS

1. La plupart des applications ne conjuguent pas encore pertinence de l'usage et maturité technologique suffisante

Les services d'attestation et de certification (*proofs of existence*), pouvant concerner **l'état civil, le cadastre, tous les contrats de type notarié ou encore des mécanismes de protection de la propriété intellectuelle**, se développent. Mais peu d'applications conjuguent, à ce jour, pertinence de l'usage et maturité technologique suffisante.

Quelques **exemples passés et actuels de ces applications** peuvent être donnés :

- **Namecoin** est ainsi un système d'enregistrement de noms de domaine qui a cherché sans succès à se substituer au système actuel « DNS » (*Domaine name system*) ;

- **Slock.it** se veut la future infrastructure majeure de l'économie collaborative ;

- **Arcade City** ambitionne de détrôner Uber en tant que plateforme de services de transport ;

- **Twister** projette de devenir le réseau social concurrent de Twitter.

La Fédération française de l'assurance estime, par ailleurs, que la technologie de la *blockchain* pourrait permettre de simplifier l'identification et la **preuve d'assurance**, ainsi que d'automatiser les procédures d'indemnisation (l'un des exemples étant l'indemnisation automatique des voyageurs en cas de retard d'avion).

Les *blockchains* pourraient, en outre, être utilisées **dans l'enseignement et la recherche** (pour la mise en place d'un registre des publications académiques par exemple) ou dans **l'action publique** plus généralement (état civil, émission de titres d'identité et de passeports, contrats de mariage, cadastre[1], organisation d'élections…). Le monopole de la

[1] *Le Ghana a ainsi expérimenté un tel stockage des titres de propriété.*

délivrance d'actes authentiques, assuré par des officiers d'état civil, des notaires ou des huissiers de justice, pourrait se trouver contesté par ces technologies.

L'application **BlockchainYourIP** vise ainsi à déposer sur un réseau de type *blockchain* des informations, sur le modèle du constat d'huissier, afin de pouvoir apporter la preuve de leur existence ou de leur antériorité. C'est, au final, toute propriété (matérielle ou immatérielle) qui pourrait être démontrée par son inscription dans un registre de ce genre. Les « contrats intelligents » ou *smart contracts* présentent eux-aussi un riche potentiel quant aux applications possibles : instruments financiers (obligations, actions et dérivés), contrats d'assurance, ventes aux enchères, crédit, loteries et jeux de hasard…

Stéphane Loignon indique que cette fonctionnalité de notarisation offre la possibilité de « *sécuriser l'information, de la graver dans un registre qui conservera la vérité des données, elle est l'outil d'une réinvention complète de l'administration publique, qui pourra fonctionner de manière transparente et efficace, comme en Estonie* ».

En janvier 2016, le *Government Office for Science*, l'organisme de conseil scientifique du gouvernement britannique, publiait ainsi un long rapport précurseur sur les possibilités offertes par la *blockchain* pour l'économie et l'État. Les auteurs y recensaient notamment les innombrables applications possibles de cette technologie pour améliorer l'action publique : « *les registres distribués peuvent aider les gouvernements à collecter les taxes, distribuer les allocations, émettre des passeports, enregistrer des titres de propriété, assurer l'approvisionnement de biens et plus généralement garantir l'intégrité des fichiers et services du gouvernement. Pour la Sécurité sociale (National Health Service – [NHS]), cette technologie permet de faire progresser les soins en améliorant et en authentifiant les services dispensés et en partageant des fichiers de manière sûre selon des règles précises. Pour les bénéficiaires de ces services, cette technologie permet, selon les circonstances, de contrôler l'accès à ses données personnelles et de savoir qui les a consultées* ».

Ce rapport préconisait aussi des expérimentations de la *blockchain* par des collectivités locales pionnières et certains services publics.

2. Les cas de l'Estonie et de Zoug

Dans cette perspective, le cas de **l'Estonie** est intéressant : la construction de cette administration numérique s'est faite en trois temps. En 2002, l'État a émis une **carte d'identité électronique**, utilisée aujourd'hui par 94 % de la population. Ce document d'identité est équipé d'une puce qui contient des clés cryptographiques permettant à son possesseur de s'identifier pour accéder à l'ensemble des services administratifs en ligne, pour voter, mais aussi pour acheter un ticket de transport ou pour récupérer une prescription à la pharmacie. La seconde étape a été **l'interconnexion progressive**, grâce à l'entrée commune offerte par cette carte d'identité numérique, de toutes les bases de données numériques des différents services de l'État.

Cette réforme, lancée dès 2001, a donné naissance au système « *X road* » (ou « carrefour ») : l'intersection de 170 bases de données publiques, offrant plus de 2 000 services à plus de 900 organisations (institutions, ministères et entreprises privées). À la demande du gouvernement, l'entreprise Guardtime a installé, en avril 2008, une **infrastructure cryptographique** équivalente à la *blockchain*, même si elle n'en portait pas à l'époque le nom. Baptisé KSI (*Keyless*

Signature Infrastructure), ce registre public distribué permet de vérifier, de manière indépendante, si une donnée a été consultée ou changée. D'après certains experts, la numérisation de ses services ferait économiser à l'Estonie 2 % de son PIB par an.

Il faut relever qu'en Suisse, depuis avril 2016, la ville de **Zoug** est devenue la première au monde à accepter les paiements en bitcoin pour ses services municipaux (certificats de naissance, acte de décès, etc.). Cette décision fait partie intégrante de la stratégie de visibilité de la ville. Cette communication vise à faire de ce territoire une sorte de Silicon Valley des cryptomonnaies, appelée « *cryptovalley* ». En réalité, seulement une dizaine d'administrés avaient réglé la mairie en bitcoins dans les six mois qui ont suivi la mise en place du service.

B. L'UTILISATION DANS LES PROCEDURES ELECTORALES ET LE VOTE

1. Un cas d'usage encore fragile

Parmi ces applications, l'une a retenu l'attention de vos rapporteurs. En effet, la *blockchain* pourrait être l'élément permettant d'organiser des systèmes de votes électroniques fiables, condition de l'avènement d'une véritable démocratie participative.

Introduite dans le droit français en 2003, la **consultation par internet n'est permise que pour les seuls Français de l'étranger**. Elle a été utilisée lors des élections législatives de 2012 et des élections consulaires de 2014.

Un rapport parlementaire des sénateurs Alain Anziani et Antoine Lefèvre a cependant souligné « *l'incapacité à concilier parfaitement la technique du vote électronique avec les principes fondamentaux de la démocratie élective : la sincérité du scrutin et le secret du suffrage*[1] ».

Louis Margot-Duclot, porte-parole en France de l'organisation Democracy Earth, explique que cette association cherche à « *donner naissance à un système de vote électronique, par une application Web facile à utiliser et à déployer, qui permettrait à ses utilisateurs d'avoir un suivi de leur vote (et donc de savoir s'il n'a pas été changé), tout en empêchant les organisateurs du scrutin de modifier ses résultats et d'avoir accès aux informations personnelles des votants* ». À cette fin, la plateforme compte s'appuyer sur la technologie *blockchain*, qui garantit l'enregistrement décentralisé de chaque vote au sein des ordinateurs du réseau. Un premier test, de portée symbolique, a été réalisé en 2016 à l'occasion du référendum colombien sur la réconciliation avec les FARC (Forces armées révolutionnaires de Colombie). Cette opération utilisait la *blockchain* du bitcoin, chaque vote étant enregistré en tant que transaction, à un coût négligeable pris en charge par l'organisation.

Toutefois, deux limites doivent être relevées : la vérification certaine de l'identité de l'électeur qui suppose toujours la médiation d'un tiers et la garantie du secret de l'isoloir.

---

[1] *Rapport d'information « Vote électronique : préserver la confiance des électeurs », par Alain Anziani et Antoine Lefèvre (n° 445, 2013-2014).*

2. Une analyse du Parlement Européen

Un rapport[1] du *Science and Technology Options Assessment* (STOA), du service de recherche du Parlement Européen, sur les perspectives de la *blockchain*, indique par ailleurs qu'en Estonie la *blockchain* a été utilisée par des actionnaires lors de conseils d'administration. Le même rapport relève une initiative similaire au Danemark, dans le cadre d'élections partisanes internes.

Selon cet organisme, la *blockchain* est susceptible de **répondre à une crise de confiance dans les démocraties modernes**. Pour beaucoup d'experts, le déploiement du vote électronique lors d'élections nationales requiert au préalable d'importantes évolutions dans les systèmes de sécurité. Il souligne cependant que l'utilisation de la *blockchain* pour le vote électronique ne se résume pas à une simple amélioration technologique. En effet, l'utilisation d'une *blockchain* publique reflète certaines valeurs qui peuvent prendre le contre-pied d'une vision traditionnelle des élections, centralisée, opaque (pour protéger l'anonymat) et « *top-down* ». L'utilisation de la *blockchain* au contraire suppose une démocratie plus directe, décentralisée et « *bottom-up* ». Ainsi, la suggestion ambitieuse a pu être faite d'utiliser de tels protocoles afin d'encourager le développement de que l'on appelle la « démocratie liquide », terme qui qualifie un système de gouvernement où les citoyens peuvent voter directement sur des orientations, ou déléguer ce pouvoir à d'autres citoyens, de manière libre et réversible.

C. DES SMART CONTRACTS POUR PROGRAMMER LA BLOCKCHAIN

1. Une définition encore peu stabilisée

Les « contrats intelligents » ou *smart contracts* sont des **programmes informatiques** inscrits dans la *blockchain.* En effet, il est possible d'échanger en son sein des lignes de script, au même titre que des transactions. Ce ne sont pas des contrats au sens juridique, mais des codes informatiques qui **facilitent, vérifient ou exécutent un contrat au stade de sa négociation ou de sa mise en œuvre**. Ainsi que l'explique le rapport de France Stratégie *Les Enjeux des blockchains*, paru en 2018[2], ces applications permettent de « *coupler la dimension transactionnelle au monde physique, ce qu'on appelle ''l'internet de la valeur''. Une transaction peut être déclenchée par une intervention directe ou par l'exécution d'un programme informatique susceptible de comporter des conditions ou des vérifications particulières, par exemple sur la date ou à partir d'informations venant du monde physique* ».

Par rapport à d'autres programmes plus classiques aux objectifs proches, les *smart contracts* présentent l'avantage de bénéficier des

---

[1] *Rapport « How blockchain technology could change our lives », février 2017, cf. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf*

[2] *http://www.strategie.gouv.fr/publications/enjeux-blockchains*

caractéristiques particulières de la *blockchain*. Ainsi, leur exécution est irrémédiable et leur code est vérifiable librement par les nœuds du réseau. Ils permettent en particulier de placer des fonds sous séquestre de manière vérifiable.

Leur mise en œuvre suppose toutefois plusieurs préalables, notamment des mécanismes de vérification approfondis, utiles en raison de l'immuabilité du registre, ainsi que le développement d'un langage de programmation adapté aux contraintes de volume de données propres à un réseau distribué.

2. La réintroduction de « tiers de confiance »

Par ailleurs, l'exécution de la plupart des cas d'usage annoncés, est **conditionnée par l'apport et l'export d'informations**. Que ce soit pour relever une température, livrer un colis, prouver la réalisation d'un travail, ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'« oracle » dans l'écosystème Ethereum, doit faire le lien entre la *blockchain* et le reste du monde, ce qui s'apparente au **retour d'un « tiers de confiance »** qui permet d'attester d'évènements au sein du monde réel, comme dans les exemples précédents.

Cette troisième fonctionnalité des *blockchains*, à travers les *smart contracts*, pourra accompagner le **déploiement des objets connectés**[1] (montres, téléphones, réveils, réfrigérateurs, voitures, etc.), de plus en plus nombreux. Ils pourraient trouver dans la *blockchain* un réseau pertinent pour communiquer entre eux, en conservant la confiance dans les informations échangées.

D. UN CONTINUUM D'APPLICATIONS ALLANT DE SIMPLES PROJETS AUX APPLICATIONS AVEREES

1. Beaucoup d'idées et encore peu de projets concrets

Parmi les applications présentées pour la *blockchain*, il est souvent difficile d'opérer une distinction rigoureuse entre les techniques selon qu'elles donnent lieu à des projets ou qu'elles restent plus ou moins en phase de développement, voire de simple idée. Très souvent, le potentiel théorique d'une

---

[1] *Voir la note scientifique de l'OPECST n°1 sur les objets connectés sur les sites du Sénat et de l'Assemblée nationale :*

https://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_2018_0013_note_objets_connectes.pdf et

http://www2.assemblee-nationale.fr/content/download/65396/664019/version/3/file/note+4+pages+objets+connectes_2.pdf

application *blockchain* fait oublier **l'absence de mise en œuvre de projets concrets.** La multiplication des protocoles de *blockchain* n'aide pas à l'essor et à la diffusion de ces applications.

2. Les *blockchains* en sont encore à un stade peu avancé

Gilles Babinet, représentant de la France sur les questions numériques auprès de la Commission européenne (*digital champion*) **relativise le stade actuel de développement des applications** : « *la blockchain, pour le moment, est un peu comme Arpanet (l'ancêtre d'internet créé en 1969) à l'égard d'internet, la technologie n'est pas encore utilisable à grande échelle, on n'a pas encore trouvé l'équivalent pour la blockchain de TCP/IP - le protocole qui a permis le passage du réseau Arpanet au réseau internet, en 1983* ».

III. LES ENJEUX MONETAIRES, FINANCIERS ET ECONOMIQUES

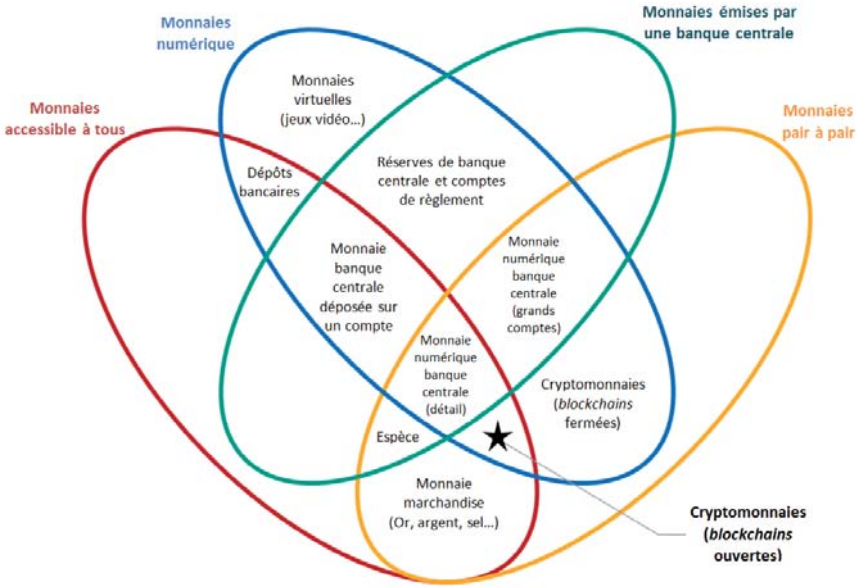
A. UNE VALORISATION DE 250 MILLIARDS D'EUROS

1. La place des cryptomonnaies parmi les autres types de monnaies

Les **enjeux monétaires, financiers et économiques** de la *blockchain* sont souvent mis au premier plan, en raison du succès notable des cryptomonnaies, surtout de la plus importante d'entre elles, le bitcoin.

Le graphique suivant, appelé « Money Flower » et utilisé par la Banque des règlements internationaux (BRI), permet de mieux comprendre **la place des cryptomonnaies parmi les autres types de monnaies**.

Les cryptomonnaies parmi les autres types de monnaies



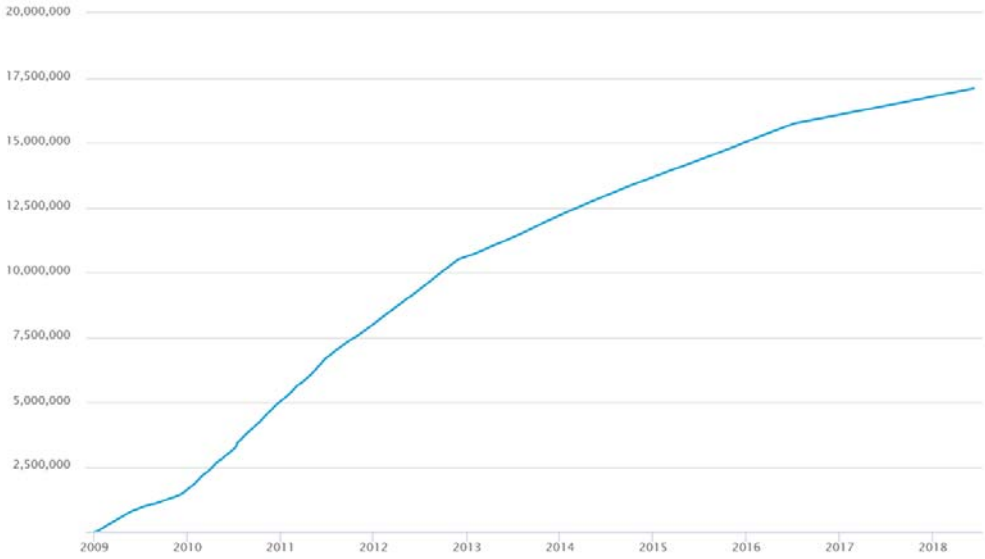
Source : OPECST d'après le chapitre « Cryptocurrencies : looking beyond the hype » *du rapport annuel 2018 de la Banque des règlements internationaux, et l'article de M. Bech and R. Garratt,* « Central bank cryptocurrencies », *BIS Quarterly Review, septembre 2017*

Des éléments chiffrés permettent de prendre la mesure de ce succès. On peut ainsi dénombrer pas moins de **17,88 millions de bitcoins** en circulation en juin 2018, dont la valeur totale est de près de **120 milliards de dollars**. Le nombre total de transactions en bitcoin par tranche de 24 heures approche les 200 000. La **capitalisation totale des cryptomonnaies** s'élève, quant à elle, à **250 milliards d'euros** ou **300 milliards de dollars**. Cette valorisation se calcule à partir des prix pratiqués par des plateformes d'échanges de cryptomonnaies, comme Coinbase aux États-Unis, Kraken en Allemagne ou la Maison du Bitcoin en France.

Les enjeux monétaires, financiers et économiques de la *blockchain*, au travers du bitcoin notamment, sont donc grandissants, d'autant que l'apparition de **nombreuses autres cryptomonnaies**, comme l'ether, le ripple, le litecoin, le conscoin, le dash, le peercoin, le neo etc. illustre un phénomène inflationniste même si ces cryptomonnaies représentent des valorisations moindres, de l'ordre de quelques dizaines de milliards de dollars au total, certaines étant inférieures au million.

2. Le cas du bitcoin

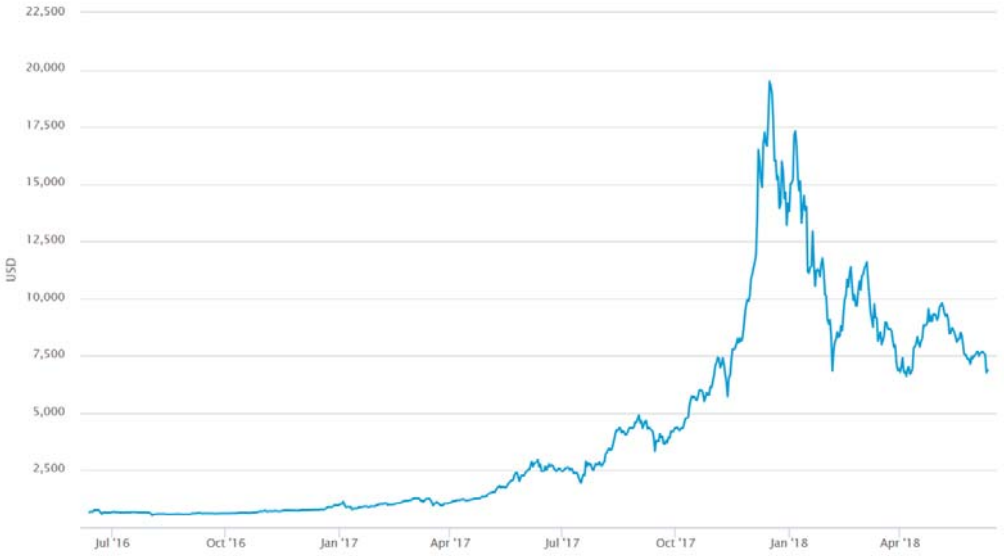
Nombre de bitcoins en circulation



Source : https://blockchain.info/charts

La valeur unitaire du bitcoin a explosé au cours de l'année 2017 et atteignait près de **20 000 dollars en décembre dernier**. Cette valeur étant en cours d'ajustement, elle est descendue à **6 876 dollars en juin 2018**.

Valeur unitaire du bitcoin en dollars



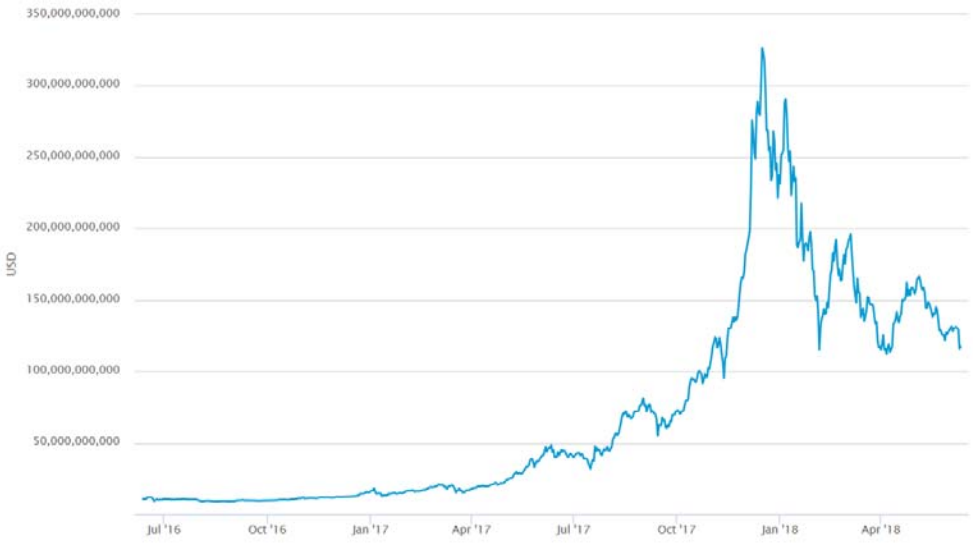
Source : https://blockchain.info/charts

Parallèlement, la capitalisation globale du bitcoin est passée en juin 2018 sous la barre des 120 milliards de dollars après avoir dépassé le stade de la valorisation à **326 milliards de dollars en décembre 2017** (plus haut historique), témoignant d'une **forte volatilité**. Selon le mathématicien Ricardo Perez-Marco, contrairement à une idée reçue, cette **volatilité est cependant en forte contraction** depuis l'émission des premiers bitcoins.

Ce constat n'empêche pas de s'interroger sur les **manipulations de cours** derrière la valorisation du bitcoin et des autres cryptomonnaies, mises en évidence par une recherche académique récente[1]. Ces phénomènes rappellent ceux existants sur les marchés financiers classiques, terrains privilégiés d'inventivité en termes de manipulations de cours mais aussi de de produits dérivés, souvent utilisés comme techniques de couverture des risques.

[1] *Cf. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066*

Valorisation totale des bitcoins en dollars



Source : *https://blockchain.info/charts*

Ces évolutions en valeur peuvent être rapprochées du poids croissant de la *blockchain* du bitcoin, soit 170 896 mégaoctets (*megabytes)*, ou **171 gigaoctets**, en juin 2018. Les éventuelles difficultés de stockage engendrées par cette augmentation, linéaire, doivent être tempérées par la hausse plus rapide des capacités de stockage informatique. Le registre Ethereum pourrait être un peu plus problématique avec une taille de **667 gigaoctets** et une croissance plus rapide que celle du bitcoin.

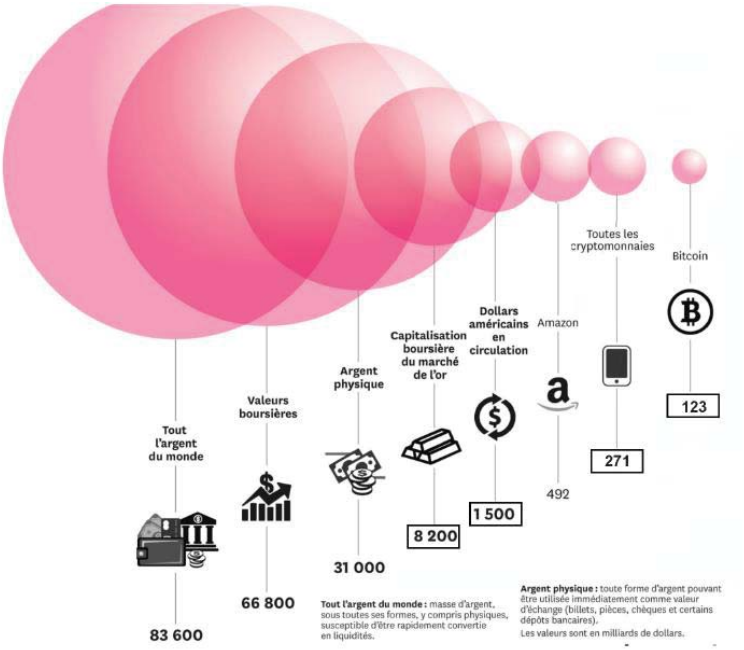
Poids de la *blockchain* du bitcoin en mégaoctets

Source : *https://blockchain.info/charts*

3. Un poids croissant qui reste à relativiser

Le **poids de la valorisation du bitcoin ainsi que celui des cryptomonnaies** dans leur ensemble est toutefois **à relativiser**, comme en témoigne le graphique suivant, dont les données remontent à l'automne 2017. Les ordres de grandeur dans les écarts constatés alors restent comparables aujourd'hui.

L'importance relative de la valorisation du bitcoin
(en milliards de dollars)



Source : Courrier international

B. LA QUESTION DES ICO (INITIAL COIN OFFERINGS)

1. Une des applications phares des *blockchains*

Une ICO (*Initial Coin Offering* ou offre initiale de monnaie) est une vente publique de jetons (*tokens*), une forme de levée de fonds non-règlementée en mode « *crowdfunding* ». Le succès de ces levées de fonds spécifiques à l'écosystème des cryptomonnaies **interroge** d'autant plus qu'elles constituent une des applications phares des *blockchains*. Elles se font moins souvent en bitcoins qu'en ethers, car ceux-ci permettent le reversement automatique de la contrepartie grâce aux *smarts contracts*.

Ces émissions d'actifs numériques (appelés jetons ou *tokens*) **échangeables contre des cryptomonnaies** ont représenté plus de 3 milliards de dollars en 2017 et représentaient un total cumulé de plus de 8 milliards d'euros en mars 2018, ce qui peut sembler peu rationnel puisqu'elles n'offrent **aucune garantie aux investisseurs**.

2. Des problèmes allant de la transparence à l'escroquerie

Elles posent des problèmes de **transparence**, **d'intérêt de l'actif** vendu, de **spéculation**, voire tout simplement d'**escroquerie**[1].

Un article récent du MIT[2] montre que près du **quart des ICO montreraient des signes visibles de fraude** : soit qu'elles aient été dénoncées par un journal spécialisé, soit que leur site web ait cessé de fonctionner après la levée de fonds, soit que cela ressorte du contenu même du « *white paper* » de présentation du projet.

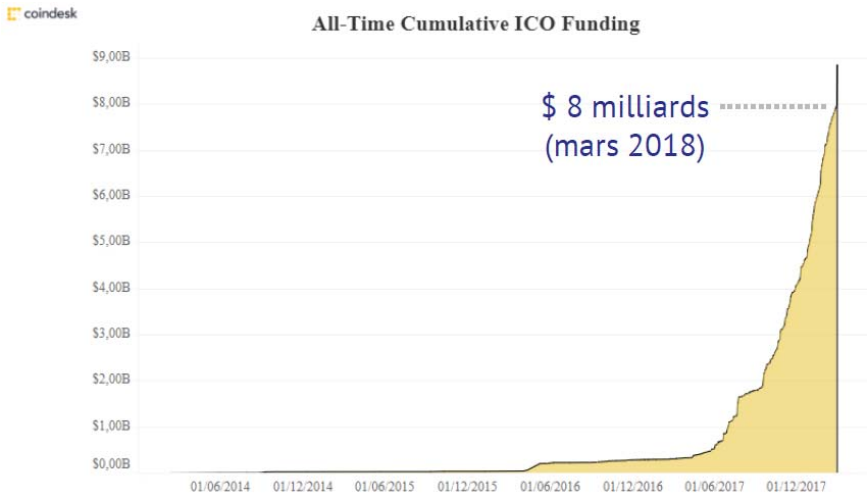
Pour ces raisons, entre autres, les entreprises Google, Facebook et Twitter ont décidé, en mars 2018, de **ne plus accepter de publicités pour les cryptomonnaies et les ICO**.

---

[1] *Le cas de la blockchain Tezos, sans constituer une escroquerie, a suscité des soupçons. Reposant largement sur des technologies françaises développées à l'INRIA, ce projet a bénéficié d'ICO aux montants records à l'époque (232 millions de dollars en 13 jours en juillet 2017, de l'ordre de 400 millions de dollars au total). Le 25 octobre 2017, une action en justice, sous la forme d'un recours collectif pour déclarations trompeuses auprès des juridictions californiennes, a visé les promoteurs et fondateurs du projet Tezos (Arthur et Kathleen Breitman et leur société américaine Dynamic Ledger Solutions, Johann Gevers, président de la fondation de droit suisse Tezos, organisateur des ICO mais également l'agence de relations publiques qui a assuré la promotion des opérations de levées de fonds Strange Brew Strategies). Cf. l'action en justice :* https://www.almcms.com/contrib/content/uploads/documents/403/4319/tezos-sfo-complaint.pdf

[2] *C.Catalini, J.Boslego et K.Zhang, «* Technological opportunity, bubbles and innovation : the dynamics of initial coin offerings *», MIT working papers.*

Le montant cumulé des ICO



Source : coindesk

3. Une opportunité nouvelle pour le financement des *start-up*

Auditionnés par vos rapporteurs, le représentant de l'entreprise française NeuroChain, Billal Chouli, et l'avocat Renaud Roquebert ont indiqué que les ICO représentent **une opportunité nouvelle pour les *start-up*** qui évoluent dans le secteur des TIC. En effet, les moyens traditionnels de levée de fonds, tels les crédits bancaires et le capital risque (*Venture Capitalism*) ne répondent que rarement à leurs besoins spécifiques (rapidité, souplesse, pari sur le long terme, forte technicité). Ainsi, le projet Neurochain s'est vu refuser certains financements au motif d'un argumentaire trop « *deep tech* » (innovations technologiques de rupture).

Les ICO, à l'inverse, permettent d'atteindre un plus large public de potentiels investisseurs. En effet, parmi ces derniers, les **motivations d'investissement** peuvent être **nouvelles** : la recherche de titres de propriété ou de retours rapides sur investissement est moins importante qu'une **volonté de parier sur l'avenir de projets innovants aux applications riches et ouvertes**.

Ces levées de fonds propres à l'écosystème de la *blockchain* permettent aussi de **s'affranchir d'une certaine réserve** exprimée par les institutions financières classiques, en particulier françaises. Certaines entreprises se heurtent ainsi, au terme d'ICO réussies, à des refus d'ouverture de compte en France, au nom de la lutte contre le blanchiment et de la fraude fiscale.

Il convient de souligner que les **ICO** devraient prochainement être **encadrées par l'Autorité des marchés financiers** (AMF), aux termes du projet de loi sur le plan d'action pour

la croissance et la transformation des entreprises (PACTE), présenté en Conseil des ministres le 18 juin 2018[1].

Au total, **les ICO doivent être regardées avec prudence** mais également sous l'angle des **perspectives de développement économique** qu'elles ouvrent.

IV. LES ENJEUX ENERGETIQUES ET ENVIRONNEMENTAUX

Comme il a été vu en première partie, les principales *blockchains* publiques, telles que Bitcoin et Ethereum reposent sur la **preuve de travail**. Elles supposent donc une **compétition mondiale de puissance de calcul** afin d'effectuer un maximum de fonctions de hachage. Ces concours de calcul sont réitérés à des intervalles donnés : soit dix minutes pour le bitcoin et quinze secondes pour l'ether. La somme gagnée par un mineur est proportionnelle à sa puissance de calcul.

Pour Jean-Paul Delahaye, le bitcoin, et cela vaut pour ses avatars, est « *comme un château gonflable pour les enfants : il ne tient que si vous dépensez sans cesse de l'électricité pour le maintenir gonflé. L'or n'a pas besoin d'être maintenu. Il tient tout seul, du fait des lois physiques* ».

Cette course se traduit par une **augmentation presque exponentielle du nombre de hashs** effectués, qui s'observe en suivant la croissance du taux de hachage (*hashrate*) des différentes cryptomonnaies. Face à l'explosion des cours, la **réduction par deux tous les quatre ans des récompenses de minage** (appelée « *halving* »)[2] prévue par le protocole de Nakamoto apparaît nettement insuffisante pour jouer son rôle de régulation de la compétition. Entre le 6 juin 2016 et le 6 juin 2018, le *hashrate* journalier du bitcoin est ainsi passé de $1{,}6 \times 10^{18}$ à 39×10^{18} hashs par seconde[3].

Ce besoin en puissance de calcul se traduit directement en une **consommation électrique considérable**. Son estimation fait l'objet de débats, mais, contrairement à ce qui est régulièrement défendu, notamment par des promoteurs du bitcoin, une **estimation minimale exprimée avec certitude est toutefois réalisable**.

---

[1] *Ce projet de loi Pacte ambitionne de donner aux entreprises les moyens d'innover, de se transformer, de grandir et de créer des emplois ; cf.* https://www.economie.gouv.fr/plan-entreprises-pacte

[2] *Le protocole de Nakamoto prévoit en effet que la récompense en bitcoin attribuée à chaque mineur validant un bloc soit divisée par deux tous les 210 000 blocs, c'est-à-dire tous les 4 ans. Elle était ainsi de 50 bitcoins jusqu'en 2012, puis de 25 jusqu'en 2016, elle est aujourd'hui de 12,5 et passera à 6,25 en 2020. Elle est versée 100 blocs après validation.*

[3] https://bitinfocharts.com/

Les *blockchains* posent donc les **questions essentielles de leurs impacts énergétiques et environnementaux**, compte-tenu des besoins considérables en électricité des *blockchains* fondées sur la preuve de travail.

A. PLUSIEURS METHODES D'ESTIMATION

Par définition, ni le nombre ni l'identité des mineurs ne sont connus, et ceux-ci ne communiquent pas sur leur consommation énergétique afin de ne pas orienter leurs concurrents. En conséquence, la consommation énergétique des principales *blockchains* ne peut que faire l'objet d'estimations, selon différentes méthodes.

Une des principales variables pour le calcul de la consommation énergétique réside dans les **écarts considérables d'efficacité entre les machines utilisables pour le hachage**.

Pendant longtemps, une simple carte graphique d'ordinateur personnel a pu suffire à miner des bitcoins, mais la situation est devenue bien différente désormais avec des calculateurs conçus uniquement à cette fin, à l'instar des circuits électroniques dédiés appelés ASIC (*Application Specific Integrated Circuit*).

Un taux de hachage de 14 terahashs/s peut ainsi être fourni par un seul appareil *Antminer S9* utilisant des processeurs ASIC d'une puissance de 1 372 W, ce qui est l'équivalent de la puissance de cacul d'un demi-million de processeurs de consoles *Playstation 3,* soit une consommation totale de 30 MW[1]. Le prix de chacune de ces machines est de 1 400 dollars sur Amazon en mai 2018.

Cet appareil, qui était le plus performant au premier semestre 2018, devrait se faire supplanter par une nouvelle génération de produits, tels que le DragonMint T1 qui contient des puces ASIC fabriquées par Samsung[2].

---

[1] *Alex de Vries, «* Bitcoin's Growing Energy Problem *», Joule 2.5 (2018) : 801-805.*

[2] *Sa puissance de 1 200 W annoncée en 2017, correspondrait en réalité à 1 480 W après des tests conduits en avril 2018, soit 13.3 Gigahashs par watt (Gh/W) annoncé et 10.8 Gh/W en réalité, soit un gain de 4 % en réalité par rapport à Antminer S9, loin des 30 % annoncés initialement.*

Un appareil *Antminer S9*

Source : wikimedia.org

L'étude de Garrick Hileman et Michel Rauchs « *Global Cryptocurrency Benchmarking Study* », conduite dans le cadre de l'Université de Cambridge en 2017, a permis de mieux saisir l'état de la situation en enquêtant directement auprès de 144 mineurs différents dans 38 pays[1].

Les *pools* de mineurs, vus en première partie de ce rapport, sont devenus de **véritables usines de calcul**, de taille impressionnante comme l'illustrent les clichés suivants. L'expression de **« ferme » de minage** prend ici tout son sens.

[1] *Cf. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf*

L'intérieur et l'extérieur d'une « ferme » de minage

Source : Kncminer

Pour calculer la consommation électrique des *blockchains*, vos rapporteurs présentent ici **trois méthodes d'estimation appliquées au bitcoin**, qui reste, de loin, la principale cryptomonnaie en termes de capitalisation. Afin d'obtenir la consommation énergétique totale de l'ensemble des *blockchains* utilisant la preuve de travail (POW), les raisonnements seraient les mêmes. Pour l'estimer, Jean-Paul Delahaye préconise de **multiplier la consommation du bitcoin par un coefficient compris entre 1,5 et 2**, afin de couvrir la consommation de toutes les cryptomonnaies utilisant la preuve de travail.

1. La méthode économique : 45 à 200 TWh/an

Cette méthode donne lieu aux **résultats les plus relayés**, car elle est utilisée par le site internet *Digiconomist*, très consulté[1]. Elle est guidée par le principe qu'un mineur est **prêt à dépenser la majorité de ce qu'il gagne** grâce à la rémunération du système en ne conservant qu'une marge.

La méthode économique de calcul de la consommation énergétique du bitcoin

Source : digiconomist.net

Les données nécessaires sont :

- le **prix du bitcoin** (que l'on nommera B) ;

- le **rapport dépense/gain jugé acceptable par un mineur** (RDG) qui doit être estimé ;

[1] *Pour suivre l'estimation du Digiconomist au jour le jour :* https://digiconomist.net/bitcoin-energy-consumption

- le **pourcentage de la dépense consacrée à acheter de l'électricité** (PE), car le mineur est aussi soumis, entre autres, à des dépenses d'infrastructure et d'entretien ;

- le **prix de l'électricité** (EL) qui peut être très variable selon les régions et pays ;

- le **revenu annuel dû aux frais de transactions** (RC) qui a pu croître jusqu'à 20 % en décembre 2017 lors du dernier grand pic du prix du bitcoin. Ici, il sera considéré comme négligeable ;

- le **coefficient d'atténuation** (CA), qui sert à anticiper ce qui va se passer dans les mois qui viennent en prenant en compte le fait que le réseau n'ajuste pas instantanément sa puissance au cours du bitcoin. Si le bitcoin vient d'augmenter. Ce coefficient sera évalué à 0,75 ou 0,5, tandis que si le bitcoin est stable ou vient de baisser, il sera fixé à 1.

Malgré sa précision, ce calcul ne prend pas en compte le fonctionnement général des fermes de minage qui est souvent opaque, l'électricité nécessaire pour fabriquer les outils de minage, qui, dans le cas du bitcoin, sont dédiés à cet usage exclusif, et l'électricité dépensée par les ordinateurs et smartphones des détenteurs de comptes qui ne participent pas directement à la gestion du réseau.

La formule à appliquer est la suivante, avec le détail des différentes étapes de sa construction.

Formule d'estimation de la consommation du bitcoin selon la méthode économique

$$\text{Conso en TWh par an} = ([B*12{,}5*6*24*365]+RC)*RDG*PE*CA/(EL*10^9)$$

- **argent gagné par an en minant :** $[B*12{,}5*6*24*365]+RC$
- **argent prêt à être dépensé pour miner :** $([B*12{,}5*6*24*365]+RC)*RDG$
- **argent prêt à être dépensé pour acheter de l'électricité :** $([B*12{,}5*6*24*365]+RC)*RDG*PE$
- **argent réellement dépensé pour acheter de l'électricité :** $([B*12{,}5*6*24*365]+RC)*RDG*PE*CA$
- **nb de KWh achetés par an :** $([B*12{,}5*6*24*365]+RC)*RDG*PE*CA/EL$
- **nb de TWh achetés par an en utilisant que 10^9 KWh = TWh :** $([B*12{,}5*6*24*365]+RC)*RDG*PE*CA/EL*10^9$

Source : Présentation de Jean-Paul Delahaye

À partir des paramètres retenus, il est possible d'effectuer **deux calculs** selon que l'on retient des hypothèses **optimistes** (d'une part, le rapport dépense/gain ainsi que le pourcentage des dépenses consacré à l'électricité sont faibles, d'autre part, le coefficient d'atténuation et le prix de l'électricité sont forts), ou **pessimistes** (à l'inverse, d'une part, le rapport dépense/gain ainsi que le pourcentage des dépenses consacré à l'électricité sont forts, d'autre part, le coefficient d'atténuation et le prix de l'électricité sont faibles).

Estimation de la consommation du bitcoin
selon la méthode économique, le 4 juin 2018

Pessimiste : B=7500 RC = 0 RDG = 1 PE = 0.60 CA = 1 EL = 0.03
Conso en TWh par an = 98.55

100 TWh

Optimiste B=7500 RC = 0 RDG = 0.9 PE = 0.40 CA = 0.8 EL = 0.05
Conso en TWh par an := 28.38

30 TWh

Source : Présentation de Jean-Paul Delahaye

Appliqué à l'ensemble des cryptomonnaies, ce mode de calcul aboutirait, selon le coefficient multiplicateur utilisé, à une valeur comprise entre 45 et 200 TWh/an (voir tableau ci-avant).

Cette méthode a l'intérêt de permettre une anticipation de la quantité d'électricité nécessaire pour la *blockchain* du bitcoin si celui-ci atteignait un certain volume financier, comme celui du dollar, ou de l'or. Ainsi l'ensemble de l'or dans le monde représentant 6 000 milliards de dollars, il faudrait multiplier la consommation du bitcoin, qui vaut aujourd'hui 127 milliards de dollars, par 50, ce qui donnerait une valeur comprise entre 1 500 et 5 000 TWh/an, soit près d'un cinquième de la consommation électrique totale mondiale (24 000 TWh).

Cependant, selon Jean-Paul Delahaye, il n'est **pas pertinent de comparer le minage de l'or à celui des bitcoins**. En effet, s'il n'est plus miné, l'or se « maintient » tout seul du fait des lois physiques. En revanche, sans un minage exigeant une consommation continue d'électricité, le système bitcoin, plus précisément sa résistance aux attaques 51 %, s'effondre.

2. La méthode « Bévand » : 60 à 80 TWh/an

Théoriquement **plus rigoureuse** car fondée sur l'évaluation de la répartition et du nombre des outils utilisés dans chaque catégorie pour atteindre la puissance du réseau, cette méthode élaborée par **Marc Bévand** n'est pas plus précise que la première car les données de base sont très difficiles à réunir et ne sont donc connues qu'avec une grande imprécision.

Cette méthode exige effectivement de connaître :

- **la puissance du réseau** et le **cours du bitcoin**, qui sont connus avec une bonne précision ;

- **le prix de l'électricité**, qui est très variable géographiquement et suppose de connaître la localisation de tous les mineurs ;

- et **la liste des outils de minage utilisés**, avec leur consommation électrique par hash produit, ainsi que **le nombre d'outils pour chaque catégorie**. Cette donnée est presque impossible à obtenir.

En mars 2017 Marc Bévand donnait une fourchette comprise entre 4,12 et 4,73 TWh/an. Sachant que depuis 2017 le taux de hachage du réseau a été multiplié par 10, tout en prenant en compte une certaine amélioration de l'efficacité des machines de minage, on obtiendrait, selon cette méthode, une consommation proche de **40 TWh/an** aujourd'hui pour le bitcoin, soit entre 60 et 80 TWh/an pour l'ensemble des cryptomonnaies (voir tableau ci-avant).

3. La méthode de calcul d'un minimum : 46,5 à 62 TWh/an

Une **estimation minimale de la consommation énergétique** peut être réalisée en partant des performances de la machine la plus efficace du marché, que l'on suppose être utilisée par l'ensemble des mineurs.

Seules deux données sont nécessaires pour réaliser le calcul :

- la **puissance du réseau** en nombre de hashs/s (soit, $36*10^{18}$ Ghashs/s le 2 juin 2018) ;

- l'**efficacité électrique de l'outil de minage le plus efficace**, aujourd'hui Antminer S9 ($13,5*10^{12}$ hashs/s pour une consommation de 1 323 W).

Il n'est pas nécessaire en revanche de connaître le prix de l'électricité ni le pourcentage de ses recettes que chaque mineur consacre à l'achat d'électricité.

Il suffit de diviser la puissance du réseau par le nombre de hashs/s produit par chaque machine, pour obtenir le nombre d'appareils nécessaires (2 666 000 unités). Puis de multiplier ce nombre par la consommation énergétique de chaque appareil, et d'extrapoler cette consommation sur une année, pour obtenir une valeur de **30,9 TWh/an**. Appliqué à l'ensemble des cryptomonnaies, cette méthode conclurait, selon le coefficient multiplicateur utilisé, à une valeur comprise entre 46,5 et 62 TWh/an (voir tableau ci-avant).

Dans la note scientifique de l'Office publiée en **avril 2018**, nous indiquions alors, avec le même calcul, obtenir une valeur de **24 TWh par an**[1]. Cette augmentation de plus de 6 TWh/an en deux mois illustre nettement **la très forte dynamique de croissance de la consommation énergétique du bitcoin** du fait de l'augmentation très rapide de la puissance du réseau.

Il convient de souligner qu'en tout état de cause ces calculs demeurent imprécis, ne prenant pas en compte tous les paramètres : ainsi l'énergie électrique de refroidissement, utilisée pour fabriquer les outils de minage et pour le fonctionnement des « mines » n'est pas prise en compte (question du PUE, *Power Usage Effectiveness*). De même, il existe un « minage pirate », qui détourne frauduleusement les capacités de calcul d'ordinateurs connectés à internet. Il est impossible d'évaluer la quantité de minage issue de ce *crypto-jacking*.

---

[1] *Note scientifique de l'Office n° 4, « Comprendre les blockchains », avril 2018.*

Synthèse des résultats de consommation énergétique obtenus selon les trois méthodes de calcul

Méthode utilisée	*Méthode économique*	*Méthode Bévand*	*Calcul minimal*
Consommation du bitcoin	30 à 100 TWh/an	~40 TWh/an	31 TWh/an
Consommation totale des blockchains publiques estimation basse (coef. 1,5)	45 à 150 TWh/an	60 TWh/an	**46,5 TWh/an**
Consommation totale des blockchains publiques estimation haute (coef. 2)	60 à 200 TWh/an	80 TWh/an	62 TWh/an
Production moyenne d'un réacteur nucléaire	7 TWh/an		

Source : OPECST, données au 2 juin 2018

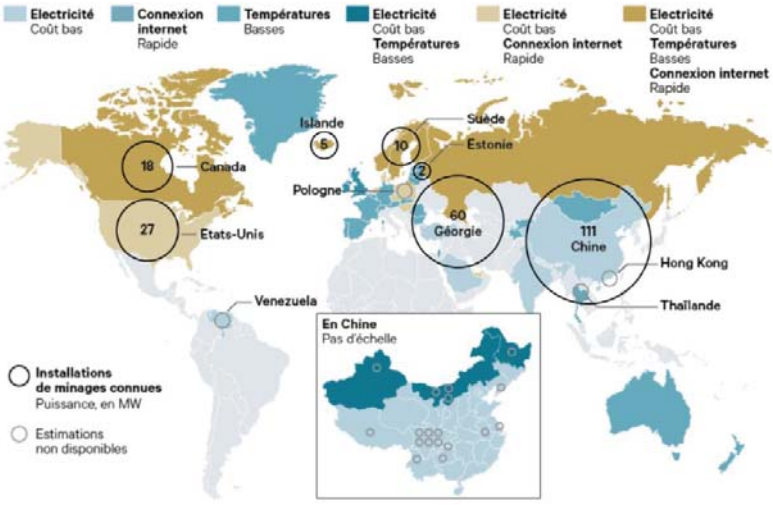
Pour mémoire, Karl J. O'Dwyer et David Malone avaient montré, dans une étude publiée en 2014, que la consommation du réseau destiné au bitcoin se situait alors dans une fourchette entre 0,1 et 10 GW de puissance électrique et qu'elle serait probablement de l'ordre de grandeur de la consommation d'un pays comme l'Irlande, soit environ 3 GW[1].

B. DES IMPACTS CONSIDERABLES, COMME L'ACCROISSEMENT MARQUÉ DES ÉMISSIONS DE GAZ À EFFET DE SERRE

L'impact en termes d'émissions de gaz à effet de serre est d'autant plus important que **les groupements de mineurs sont surtout établis en Chine**, pays qui présente pour sa production électrique **l'intensité carbone la plus élevée au monde**. La Chine présente en effet, selon les calculs du GIEC, une intensité carbone de 1 050 grammes de CO_2 par kWh d'électricité produite.

Estimation de la répartition des mineurs de bitcoin dans le monde

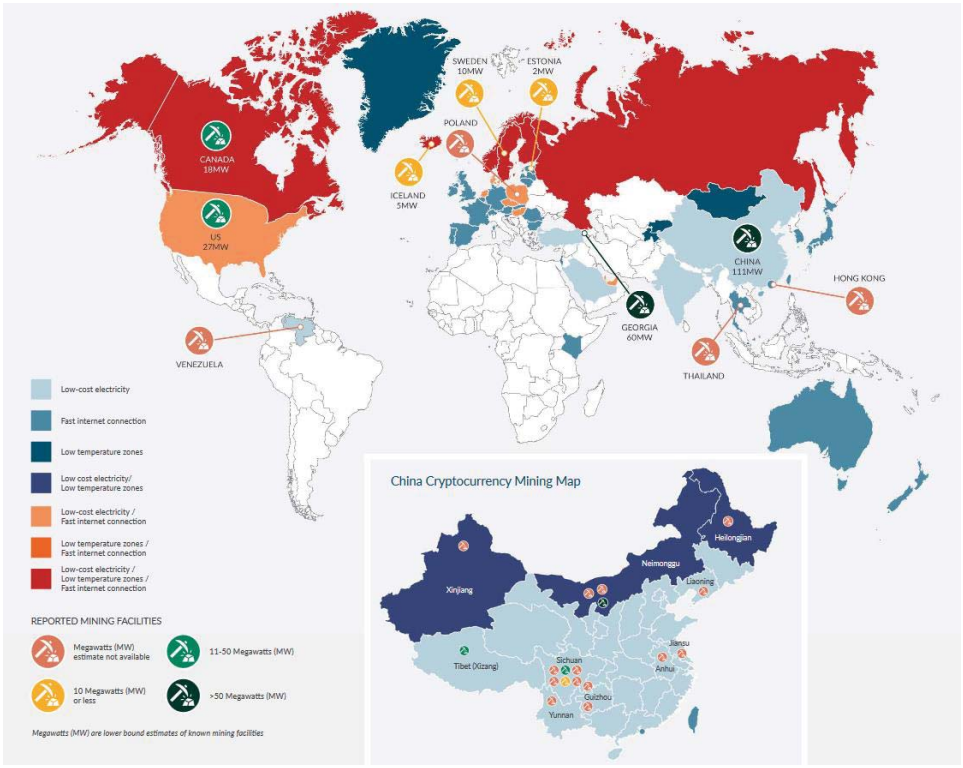
[1] *Cf. https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf*



Source : présentation de Jean-Paul Delahaye

Ces phénomènes de concentration géographique s'expliquent surtout par les **écarts de coût de l'électricité selon les États**. La Chine offre ainsi **l'électricité la moins chère**, souvent dans des zones où des barrages hydro-électriques ont été construits pour anticiper des arrivées massives de nouveaux habitants ou l'implantation de villes nouvelles, qui ont été moindres que prévues, permettant à des activités industrielles de profiter d'une énergie à moindre coût.

Coût de l'électricité et consommation par État



Source : Garrick Hileman et Michel Rauchs, Global Cryptocurrency Benchmarking Study, Université de Cambridge[1]

Au-delà même d'un impact environnemental certain, démontrant les importantes externalités négatives de ces technologies, les *blockchains* utilisant la preuve de travail ont déjà pu poser des **difficultés d'approvisionnement au niveau local**.

Ainsi en février 2018, la ville de **Plattsburg** dans l'État de New-York a interdit pendant 18 mois l'installation de nouvelles usines de minage, car leur présence avait fait augmenter le prix de l'électricité pour les usagers[2]. Une amende de 1 000 dollars par jour de violation du moratoire a alors été imposée aux mineurs.

---

[1] *Cf.* https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

[2] *Cf. «* Small towns try to tame the bitcoin boom *», Citylab.com, mars 2018, lien :* http://www.citylab.com/life/2018/03/small-towns-try-to-tame-the-bitcoin-boom/556298/

En avril, les forces de police de la **Corée du Sud** ont procédé à l'interpellation de 14 mineurs de bitcoin utilisant illégalement de l'électricité à bas prix destinée à l'industrie classique[1].

Il est à noter ici que le minage peut avoir d'autres effets néfastes qu'une consommation énergétique importante, notamment en mettant en tension le marché de certains matériels informatiques. Ainsi, Ethereum nécessitant des **cartes graphiques** pour effectuer sa preuve de travail, le prix voire même la disponibilité de celles-ci à l'échelle mondiale ont été affectés par la hausse du cours de l'éther[2]. Plusieurs cas de difficultés d'approvisionnement ont été évoqués devant vos rapporteurs et le doublement, voire le triplement, du prix des cartes graphiques Nvidia GTX 1060 ainsi que des processeurs AMD RX 570 et 580 a été constaté sur quelques mois.

Quant aux **millions d'appareils de hachage** conçus pour produire du bitcoin, ils deviennent **rapidement obsolètes** lorsqu'ils sont remplacés par de nouvelles versions plus puissantes, et ne peuvent être réutilisés à une autre fin. Cela représente un **gaspillage difficilement soutenable de matériel** peu recyclable.

C. VRAIES ET FAUSSES SOLUTIONS D'UN PROBLEME QUE LA RECHERCHE DOIT CONTRIBUER A RESOUDRE

Il est régulièrement avancé que la consommation énergétique diminuera avec l'augmentation des capacités de calcul, l'utilisation d'électricité surproduite ou la réutilisation de la chaleur engendrée par le fonctionnement des fermes. **Ces arguments ne sont pas valables** car ils ne tiennent pas compte du fait que la compétition entre les mineurs ne joue pas sur la consommation d'énergie mais sur les coûts de celle-ci.

En ce qui concerne l'augmentation des capacités de calcul par le progrès des circuits dédiés ASIC, tels *Antminer S9*, celle-ci concerne l'ensemble des mineurs et des attaquants. Les économies offertes aux mineurs le sont aussi aux attaquants potentiels. Par ailleurs, si les mineurs revendent de l'énergie sous forme de chaleur ou utilisent de l'énergie verte moins onéreuse, ils libèreront des fonds pour augmenter leur puissance totale de calcul, et leur consommation d'électricité continuera donc à augmenter.

Pour vos rapporteurs, la consommation énergétique excessive des cryptomonnaies est directement liée à l'utilisation de la preuve de travail.

Seul le passage à une autre méthode de consensus semble être une solution viable à ce qui représente un obstacle social, environnemental et politique au développement des technologies de *blockchains*. Comme il a été évoqué dans la première partie de ce rapport (voir III, B-2), cette transition n'est cependant pas sans poser de sérieuses difficultés techniques.

---

[1] *«* Fourteen people from 13 companies have been arrested for illegally using cheap electricity to mine cryptocurrencies at industrial complexes in South Korea *», Coindesk.com, avril 2018.*

https://www.coindesk.com/korean-police-bust-bitcoin-miners-illegally-using-cheap-factory-power/

[2] *https://www.tomshardware.com/news/ethereum-effect-graphics-card-prices,34928.html*

La recherche doit donc **relever ce défi de la consommation énergétique**, à l'image de l'initiative française BART[1] (« *Blockchain* Advanced Research & Technologies »). Ce programme s'intéresse notamment à une méthode de validation des blocs consommant moins d'énergie, tout en utilisant des méthodes de consensus robustes aux moyens cryptographiques avancés, en développant de nouvelles architectures assurant la fiabilité et accompagnant la montée en charge du réseau.

Au-delà de la sécurité et de la consommation énergétique, les *blockchains* posent des questions de fond aux **autorités politiques** et, plus généralement, au grand public, à travers les problématiques de protection des données personnelles, de cadre juridique, de régime fiscal ou, encore, de souveraineté.

V. LES ENJEUX JURIDIQUES

En raison de leurs caractéristiques d'immuabilité, de distribution globale et de libre participation, les *blockchains* **publiques posent des questions inédites aux législateurs nationaux**. Celles-ci portent notamment sur le régime fiscal, le cadre juridique ou la protection des données personnelles. Si des alternatives se développent ou sont annoncées, **aucune *blockchain* publique populaire ne semble aujourd'hui en mesure de lever tous les obstacles juridiques révélés par le bitcoin**.

Parmi les acteurs qui se sont saisis de la question, la Commission nationale de l'informatique et des libertés (CNIL) a lancé une mission prospective il y a plus de 18 mois pour anticiper les questions de conformité légale des solutions utilisant des *blockchains*, en particulier vis-à-vis des exigences du Règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai dernier. Toutefois, comme l'a démontré l'audition par vos rapporteurs de plusieurs de ses responsables, elle **réserve encore aujourd'hui ses conclusions**, tant la question de la protection des données personnelles, liée à l'anonymat ou au pseudonymat sur les *blockchains* publiques, semble complexe à traiter.

D'autres acteurs, en particulier des avocats et professionnels du droit, sont très enthousiastes quant aux potentialités offertes par les technologies *blockchains*. Ils évoquent notamment son intérêt en termes de simplicité d'audit et d'automatisation des contrats, reprenant à leur compte les théories de Lawrence Lessig sur le « *code is law* »[2]. En matière de contentieux, ils relèvent l'importance d'une preuve inscrite dans la *blockchain* et estiment qu'il y a là sujet à réflexion. Ils notent une évolution probable du métier de juriste, qui devra s'adapter aux problématiques nées de la *blockchain*. Pour répondre aux demandes des clients qui souhaitent avoir un éclairage sur la conformité de leur utilisation de la *blockchain* à la loi, ils doivent se former techniquement. Ils devront par exemple analyser un *smart contract* pour certifier qu'il réalisera bien l'opération envisagée, ou même à en rédiger.

---

[1] *Cette initiative commune de recherche réunit l'INRIA, Télécom ParisSud, Télécom ParisTech et SystemX. Lancée le 6 mars 2018, sa feuille de route comprend des recherches sur les modèles théoriques, le passage à l'échelle et le monitoring, la sécurité de bout en bout, les architectures, la confidentialité des données, les modèles économiques et la régulation, l'impact social et le passage à d'autres modes de preuve.*

[2] *Lawrence Lessig, « Code et autres lois du cyberespace », 1999.*

Cependant, certains mettent en garde contre de **nouveaux risques**, comme ceux relevant de l'« obfuscation », c'est-à-dire la publication intentionnelle d'informations fausses, sans possibilité évidente d'effacement.

Parmi les problèmes juridiques que pose plus spécifiquement le développement du bitcoin, on relève en particulier des risques liés au **blanchiment et au financement du crime organisé**, sa confrontation aux exigences en matière de **protection des données personnelles**, mais aussi plus récemment, le **risque de diffusion de contenus illicites**.

Un certain nombre d'acteurs mettent aussi en avant les questions liées à la **qualification fiscale complexe des cryptomonnaies** et de certaines activités liées aux *blockchains*, en particulier les **ICO**.

A. FRAUDES, CADRE JURIDIQUE DEFAILLANT ET REGIME FISCAL FLOU

Les **enjeux juridiques** de la *blockchain* sont considérables. Le régime fiscal des cryptomonnaies est le point le plus débattu mais le statut des transactions opérées via la *blockchain*, la valeur juridique des *smart contracts*, l'**opacité** des opérations menées souvent sous couvert d'anonymat, sont autant de sujets qui demeurent en discussion. Il faut souligner qu'un groupe de travail sur les normes ISO de la *blockchain* a été lancé l'année dernière.

1. Activités frauduleuses

Les risques d'**utilisation frauduleuse** du bitcoin à des fins de financement d'activités illégales (crime organisé, trafic de stupéfiants…) sont probablement parmi les plus commentés. Toutefois le poids des cryptomonnaies rapporté à l'ensemble des revenus du crime organisé (de l'ordre de 900 milliards de dollars par an) est à **relativiser**.

Il est possible de vendre et d'acheter des bitcoins partout dans le monde, leur utilisation pour une éventuelle conversion en monnaie classique ne dépendant que de la possession de clés privés et d'une plateforme d'échange dédiée. Ces clés peuvent être inscrites sur un support physique (un « portefeuille » physique sécurisé, une carte mémoire ou une feuille de papier), et donc très aisément franchir une frontière en échappant à tout contrôle. Un grand nombre d'experts estiment toutefois que le bitcoin serait de plus en plus **délaissé par les auteurs d'activités illicites**, celui-ci étant de moins en moins considéré comme réellement intraçable[1].

En ce sens, la transparence totale des échanges et l'indestructibilité de l'historique des transactions pourraient être considérées comme un avantage du bitcoin par rapport à des systèmes plus centralisés, du point de vue des pouvoirs publics qui pourraient alors plus facilement exercer une surveillance.

---

[1] *Cf. Reid F., Harrigan M., «* An Analysis of Anonymity in the Bitcoin System *», 2011 IEEE* International Conference on Privacy, Security, Risk, and Trust. *Le 20 mars 2018, The Intercept, média d'investigation américain travaillant à partir des révélations d'Edward Snowden, révèle que la NSA a identifié et suivi l'activité d'un grand nombre d'utilisateurs du bitcoin, dans le cadre d'un programme appelé MONEYROCKET.* https://theintercept.com/2018/03/20/the-nsa-worked-to-track-down-bitcoin-users-snowden-documents-reveal/

2. Insertion de données illégales

Si l'objet premier du bitcoin reste financier, il est possible dans une certaine mesure d'intégrer dans un bloc des **données non-financières**[1]. C'est l'objet en particulier d'une fonction appelée *OP-return* qui permet d'insérer quelques bits (80 octets) d'informations non transactionnelles dans chaque transaction d'un bloc. Lorsque celui-ci est validé, ces informations sont alors téléchargées par l'ensemble des nœuds. Or ces données peuvent être illicites, comme l'a montré une étude publiée en mars 2018 par des chercheurs allemands[2]. Ils ont révélé que la *blockchain* du bitcoin contenait un certain nombre de fichiers ou de liens vers des fichiers de nature non financière. On y trouve ainsi des documents, ou leurs hashs, soumis à la propriété intellectuelle, des informations privées (courriels, photographies…), du contenu politique sensible ou un logiciel d'assistance à la contrefaçon, mais aussi des liens renvoyant vers des sites pédopornographiques. À ce titre, chaque possesseur de la *blockchain* du bitcoin, c'est-à-dire chaque nœud, est **potentiellement dans l'illégalité dans de nombreux pays**.

3. Fiscalité

La problématique du **« flou » fiscal** entourant les activités touchant à la *blockchain* pose en fait la question du **statut des cryptomonnaies** : doivent-elles être considérées comme des monnaies ou des biens ? De la réponse à cette question dépend leur exonération ou non de la taxe sur la valeur ajoutée (TVA). Un arrêt de la Cour de justice de l'Union européenne (CJUE) en date du 22 octobre 2015 considère le bitcoin comme un « moyen de paiement » et a donc décidé d'exonérer ses échanges de TVA, invalidant une interprétation du fisc suédois.

En France cependant **ce statut reste peu clair**[3], si bien que le fisc, ainsi que les douanes et les autorités financières, comme l'Autorité des marchés financiers (AMF) ou l'Autorité de contrôle prudentiel et de résolution (ACPR), n'ont pas encore exactement déterminé quelle réglementation appliquer aux cryptomonnaies ni su toujours définir leur propre champ de compétence[4].

Sur cette question, des **travaux parlementaires sont en cours** : d'une part, la commission des Finances du Sénat, qui s'intéresse depuis 2014 à ce sujet, a conduit à nouveau

---

[1] *Cf. pour une recension récente des méthodes d'insertion de données arbitraires dans la blockchain du bitcoin, A.Sward, I.Vecna et F.Stonedahl, «* Data Insertion in Bitcoin's Blockchain *», 2018, dans le Ledger Journal, https://ledgerjournal.org/ojs/index.php/ledger/article/view/101/93*

[2] *Cf. Matzutt et Hiller «* A quantitative analysis of the impact of arbitrary blockchain content on bitcoin *»,* Financial Cryptography and Data Security International Conference*, 2018, http://fc18.ifca.ai/preproceedings/6.pdf?utm_source=JeromeVosqienFR&utm_medium=SophosFranceLink*

[3] *Il faut cependant mentionner la décision du Conseil d'État d'avril 2018 : http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/Conseil-d-Etat-26-avril-2018-M.-G-et-autres*

Voir aussi : https://bitcoin.fr/la-decision-tant-attendue-du-conseil-detat-vient-detre-rendue/

[4] *« Quelle est la nature juridique de Bitcoin ? », Bitcoin.fr, 30 octobre 2015.*

des auditions en 2018[1] ; d'autre part, la commission des finances de l'Assemblée nationale a mis en place une mission sur les cryptomonnaies, présidée par Éric Woerth et dont le rapporteur est Pierre Person.

4. Régime de responsabilité

Une dernière interrogation fondamentale concerne la **responsabilité** : qui l'endosse lorsqu'un litige survient dans l'utilisation d'une application fonctionnant sur une *blockchain* publique ? Est-ce celui ou ceux qui ont créé le protocole de *blockchain*, conçu l'application utilisée, ou l'ensemble de la communauté des membres, c'est-à-dire tous les nœuds, ce qui en pratique est impossible ?

Faut-il alors se tourner vers le créateur de l'application, ou ses utilisateurs ? La logique de la *blockchain* est de faire reposer la confiance des utilisateurs non pas sur un organisateur central mais sur un code dont la lecture est ouverte à tous. Pour Nicolas Courtois, cette pratique courante en informatique s'apparente à un « *far west* ». En effet, puisque l'utilisateur peut être la victime d'un code qu'il n'a pas les moyens d'auditer ni même de comprendre.

Les experts britanniques du *Government Office for Science* proposent une piste intéressante quoiqu'ambitieuse à destination des pouvoirs publics, il s'agirait d'intervenir non pas dans la loi, mais dans le code lui-même : « *le code technique, y compris les logiciels et les protocoles, peut émerger du secteur public. TCP/IP par exemple, ainsi que d'autres protocoles fondamentaux d'internet, sont issus de projets de recherche financés par des gouvernements et désormais supervisés par l'Internet Society, une ONG internationale […]. Ce n'est pas une solution parfaite, mais cela montre la possibilité d'une implication publique et d'une représentation démocratique dans la production de code – une régulation publique par le code informatique plutôt que par le code juridique*[2] ».

Il est certain que « *la plupart des pays développés se mobilisent et expriment une volonté accrue de contrôler les pratiques frauduleuses liées à l'usage des blockchains* »[3] , ainsi qu'en témoigne la mise à l'ordre du jour, à la demande de la France, de ce sujet lors d'un sommet du G20 en mars 2018[4]. Une série de recommandations du Groupe d'action financière

---

[1] *Auditions du 7 février 2018 sur les nouveaux usages et la régulation des chaînes de blocs (blockchains) et sur les risques et enjeux liés à l'essor des monnaies virtuelles. En 2014, la commission des finances du Sénat avait rendu un rapport intitulé « La régulation à l'épreuve de l'innovation : les pouvoirs publics face au développement des monnaies virtuelles » (rapport d'information n° 767, 2013-2014).*

[2] United Kingdom Government Office for Science, « Distributed Ledger Technology: beyond blockchain *», 2016, cf. le rapport au lien suivant :*

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[3] *Cf. le rapport de France Stratégie «* Les Enjeux des blockchains *» :*

http://www.strategie.gouv.fr/publications/enjeux-blockchains

[4] *Cf. https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf*

(GAFI), ou en anglais *Financial Action Task Force* (FATF), avait été adressée en amont aux participants à la réunion[1].

Les **failles juridiques de la *blockchain* semblent pouvoir être résolues par des solutions techniques**, toutes cependant supposent une forme de **transparence** de la *blockchain* et de connaissance des utilisateurs. Or, cette transparence semble en contradiction frontale avec les solutions techniques apportées à la question de la protection des données personnelles.

B. LA PROTECTION DES DONNEES PERSONNELLES

Selon l'avocat Jérôme Deroulez, « *Le développement de la blockchain – comme la multiplication de ses cas d'usages – pourrait s'avérer un frein à la montée en puissance du droit à la protection des données personnelles du fait de ses caractéristiques techniques. Cette technologie pourrait également être entravée ou limitée du fait de réglementations peu incitatives, en réponse à des dérives régulièrement critiquées (anonymat, blanchiment, fraude etc.)* » [2].

1. La *blockchain* est-elle compatible avec le RGPD ?

La protection des **droits sur les données personnelles** inscrites sur la *blockchain* du bitcoin se pose avec une acuité particulière avec l'entrée en vigueur le 25 mai 2018 du *Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (RGPD) qui s'applique au traitement automatisé de données à caractère personnel. Ce règlement vient en effet consacrer, d'une part, l'identification d'un responsable de traitement[3], d'autre part, **le droit à la rectification**[4] **et le droit à l'oubli**[5], deux exigences qui sont par essence contradictoires avec un système de *blockchain* immuable et purement pair à pair.

En effet, selon Daniel Augot « *Sur les blockchains publiques, toutes les données inscrites sont en standard lisibles et la notion de pseudonyme, proposé par exemple par Bitcoin et Ethereum, est très faible en pratique, la désanonymisation d'une entité de ces protocoles est relativement facile* ». Par ailleurs, les données envoyées dans un réseau de *blockchain* sont inscrites dans plusieurs milliers de serveurs indépendants les uns des autres et répartis tout autour du globe, ce qui revient à les rendre rapidement ineffaçables.

La position de la CNIL est de ne pas considérer la *blockchain* comme un traitement en soi, mais seulement les applications qui fonctionnent avec des *blockchains*, de façon à permettre une meilleure identification du responsable de traitement. En ce qui concerne les

---

[1] *Cf. http://www.fatf-gafi.org/media/fatf/documents/FATF-G20-FM-CBG-March-2018.pdf*

[2] *J. Deroulez, « Blockchain et données personnelles, quelle protection de la vie privée ? », 18 septembre 2017, Semaine Juridique édition générale n° 38.*

[3] *Article 4 alinéa 7 du RGPD.*

[4] *Article 16 du RGPD.*

[5] *Article 17 du RGPD.*

droits personnels sur les données, garantis par le RGPD, elle invite les développeurs d'applications à réfléchir à des systèmes prévoyant le masquage des informations envoyées sur une *blockchain* publique. En revanche, elle reconnaît que, dans certains cas, le droit à l'oubli, tout comme l'interdiction de transfert des données en dehors du territoire de l'Union Européenne, ne pourront être protégés qu'avec des innovations techniques au niveau des protocoles eux-mêmes.

2. Quelques solutions techniques envisageables

Si des initiatives de membres de la communauté Bitcoin ont vu le jour pour renforcer la protection de la vie privée[1] en garantissant **un système anonyme qui échapperait aux exigences réglementaires**, celles-ci ne font pas l'unanimité tant elles s'éloignent de la transparence chère aux premiers promoteurs de la technologie. De nombreuses réponses techniques sont envisagées, qu'elles prennent la forme de modifications apportées aux protocoles existants ou de nouvelles solutions (il a été vu que l'une et l'autre pouvaient se succéder dans le cas d'une *hard fork*, une mise à jour non adoptée à l'unanimité pouvant donner naissance à deux réseaux distincts).

Pour garantir l'anonymat d'une transaction sur la *blockchain*, la solution la plus simple reste de multiplier les adresses (clés publiques) utilisées. Cela peut se faire manuellement pour le bitcoin, ou automatiquement avec des outils comme Paymium, mais ces solutions ne sont pas à l'abri d'un recoupement[2]. De manière plus élaborée, il est possible de s'en remettre à un service de « mixage », qui propose, moyennant rétribution, de multiplier les échanges intermédiaires entre un émetteur et un récepteur. Ces services sont cependant assez peu utilisés car ils supposent de faire une grande confiance au tiers qui en a la charge[3].

Bien plus avancées, des techniques cryptographiques permettent de **prouver l'existence d'une transaction sans en révéler le contenu**. Il s'agit en particulier des zk-SNARKs (« *zero knowledge succinct non-interactive argument of knowledge* »), qui sont des preuves dites en anglais « *zero knowledge* » et en français « sans divulgation de connaissance ». Elles permettent de fournir une preuve qu'un énoncé (une transaction) est juste, sans rien révéler du contenu de la preuve. Ainsi, on peut poster des « preuves *zero knowledge* » de validité des transactions, sans dévoiler l'émetteur, le destinataire ou les montants engagés. Elles supposent toutefois que des paramètres spécifiques aient été créés par une entité de confiance.

Des cryptomonnaies sont ainsi entièrement dédiées à **l'anonymat des transactions**. On peut citer Monero (basée sur le principe de la « signature de cercle ») ou Zcash (fondée sur le principe de preuve sans divulgation de connaissance), qui se classaient en avril 2018 parmi les trente cryptomonnaies les plus importantes en termes de capitalisation. Ces processus nécessitent toutefois des temps de calcul particulièrement importants, jusqu'à 1 000 fois plus

---

[1] *Technique de « mixage » des bitcoins, cf. coinmixer.se*

[2] *F.REID et M.HARRIGAN "An Analysis of Anonymity in the Bitcoin System", 2011, IEEE International Conference on Privacy, Security, Risk, and Trust.*

[3] *De tels mixeurs, qui ne nécessitent pas de confiance, font toutefois l'objet de recherches, cf. https://github.com/BUSEC/TumbleBit/*

longs que ceux du bitcoin, qui ne permettent pas encore d'envisager leur utilisation pour un grand nombre d'usages, en particulier non-financiers.

Des projets se proposent de répondre à ces contraintes liées au recours à la *blockchain* en l'**absence de confidentialité** lors des transactions. C'est le cas du projet *Hawk*[1]. Pour favoriser l'utilisation des *smart contracts* et de ces protocoles informatiques, par exemple dans le domaine des assurances ou des transactions financières, ses auteurs proposent d'éviter que certaines informations touchant à la vie privée puissent être visibles par les autres utilisateurs sur une *blockchain,* en recourant notamment au mécanisme de preuve à divulgation nulle de connaissance.

Le programme de recherche *TRUST* du *Massachusetts Institute of Technology (MIT)* comprend un projet appelé *ENIGMA*, élaboré par Guy Zyskind[2], qui vise à permettre l'échange de données privées voire sensibles sur des réseaux de *blockchains*, sans atteinte à la vie privée. Guy Zyskind assure que ce projet « *permet de traiter des données sans les voir* ». Une thèse de doctorat est conduite sur ce sujet, dans le cadre du projet BART.

3. Des solutions insuffisantes

Toutefois si des solutions techniques, d'une part, au problème de l'anonymat, d'autre part, au contrôle des utilisations et insertions frauduleuses, sont développées voire en fonctionnement, **peu arrivent à réunir les deux objectifs**. Il faut ici relever l'exception notable des *blockchains* à accès restreint (ou « privées ») qui, parce qu'elles reposent sur une forme de gouvernance centralisée, permettent l'identification d'une entité responsable (qui peut prendre la forme d'un consortium) et contrôlable.

Vos rapporteurs restent toutefois sceptiques quant à la possible émergence d'une *blockchain* publique qui soit respectueuse des exigences du RGPD et soumise au contrôle du régulateur. Selon Daniel Augot, « o*n retrouve ici l'opposition classique entre la préservation de la vie privée et les préoccupations sécuritaires des États (qui veulent contrôler les flux) ».* Pour lui, cette opposition d'ordre juridico-politique pourra être dépassée grâce à la recherche[3]. Selon le chercheur Georg Fuchsbauer, non seulement l'anonymat permet de protéger la vie privée, mais il évite que des mineurs puissent pénaliser un utilisateur identifié en refusant de valider ses transactions.

---

[1] *Cf. A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk : the blockchain model of cryptography and privacy-preserving smart contracts, juin 2015 ; https://eprint.iacr.org/2015/675.pdf. Ils recourent aux travaux de L. Patey, Preuve à divulgation nulle de connaissance : Institut de recherches en informatique fondamentale, 2009, le projet https://www.irif.fr/~carton//Enseignement/Complexite/ENS/Redaction/2009-2010/ludovic.patey.pdf*

[2] *Porté par Guy Zyskind, Oz Nathan et Alex Pentland, ce programme cherche à répondre aux enjeux posés par l'explosion des données en créant des cadres techniques et juridiques globaux. Cf. le projet ENIGMA du MIT, www.media.mit.edu/projects/enigma/overview/ et le programme TRUST : www.trust.mit.edu/ Cf. aussi G. Zyskind, O. Nathan, A. Pentland, White paper.Decentralizing Privacy : Using blockchain to protect personal data, www.enigma.co/ZNP15.pdf*

[3] *Cf. https://eprint.iacr.org/2016/061*

Les solutions techniques à ces obstacles juridiques semblent en effet remettre en cause les caractéristiques les plus fondamentales des *blockchains*, qui ont fait leur succès auprès d'utilisateurs désireux d'échapper à une régulation, étatique ou privée, considérée comme arbitraire.

Jérôme Deroulez se veut cependant optimiste car « e*n dépit d'un mode de fonctionnement parfois antinomique avec les principes du droit à la protection des données, la blockchain apportera peut-être paradoxalement les solutions techniques les plus à même de protéger ces données à l'ère du numérique et de garantir l'effectivité d'un droit parfois mis à mal dans un environnement technologique de plus en plus complexe et transnational* ».

VI. DES ENJEUX DE SOUVERAINETE ?

A. LA GEOPOLITIQUE DU MINAGE

Les **phénomènes de concentration géographique** des fermes de minage, vus précédemment, soulèvent des **questions d'ordre géopolitique**. Avec plus de 60 % des fermes de minage établies sur son sol, la **Chine** pourrait ainsi chercher à **déstabiliser** telle ou telle cryptomonnaie, à commencer par le bitcoin, avec des effets majeurs. La **Russie**, de son côté, a choisi d'encourager l'implantation de *pools* de mineurs car elle y voit un intérêt stratégique.

L'utilisation des *blockchains*, à travers le minage notamment, pose la question du **rôle de l'État** et **le principe de souveraineté**. La *blockchain* pourrait aussi redistribuer les cartes du pouvoir à l'échelle mondiale. Comme l'explique l'entrepreneur Frédéric Montagnon, fondateur de Legolas : la *blockchain* pourrait remettre en cause la domination américaine et serait « *une occasion unique, un nouveau protocole de l'internet que les géants d'aujourd'hui ne contrôlent pas. Si l'on veut concurrencer un jour Facebook et Google, on peut désormais le faire avec des millions de petites briques, de petits projets, qui se financeront en lançant des millions de monnaies* ».

B. UNE LOGIQUE MONOPOLITISQUE

La **compétition des protocoles** *blockchain* devrait progressivement céder le pas à une **logique plus monopolitisque**. Stéphane Loignon observe ainsi que « *la centralisation quasi-monopolistique est en effet devenue la règle dans l'économie numérique. Dans tous les services qui mettent en relation l'offre et la demande, un acteur dominant, voire ultradominant, a émergé : les moteurs de recherche et la messagerie (Google), le commerce électronique (Amazon), les réseaux sociaux (Facebook), le Web mobile et la vente de musique (Apple), la mise en relation avec des chauffeurs (Uber), la location de logements (Airbnb)…* ».

L'économie numérique a en effet connu quatre grandes vagues, qui ont chacune fait émerger leurs champions : d'abord celle des moteurs de recherche, des messageries et du commerce électronique, incarnée par les géants Google (fondé en 1998) et Amazon (dès 1994) ; ensuite, celle de réseaux sociaux et de l'internet « 2.0 » (participatif), symbolisée par Facebook ou Twitter (respectivement créés en 2004 et 2006) ; puis, celle de l'économie collaborative (ou « du partage »), dont les fers de lance ont été Airbnb (2008) et Uber (2009) ; enfin, celle du cloud ou de « l'informatique dématérialisée », un marché que se sont partagé des géants déjà installés (Amazon, Google, Microsoft et IBM) et quelques nouveaux entrants (Dropbox, créé en 2008).

Une cinquième vague est peut-être en train de se former avec la *blockchain*, dans la mesure où elle pourrait conduire à restructurer l'ensemble des industries et des services issus des quatre premières vagues, sur un mode désormais désintermédié.

Selon le rapport de France Stratégie « *Les Enjeux des blockchains* »[1], « *dans la banque, l'assurance, mais aussi la logistique ou la santé, la technologie de la blockchain pourrait provoquer une véritable mutation dans la chaîne de valeur. Les plateformes numériques, qui sont des systèmes centralisés, ne sont pas à l'abri : championne de la désintermédiation, la blockchain a pu être décrite comme un moyen d' "ubériser Uber"* ». Pour Pierre Noizat, fondateur de Paymium, « *la décentralisation des serveurs est un enjeu majeur économique et démocratique. Économique d'abord, car aujourd'hui, un serveur central (toujours américain) capture toutes les données dans chaque secteur : Amazon, Apple, Uber, Google… La valeur ajoutée est ainsi aspirée dans la Silicon Valley* ».

Nicolas Courtois, professeur de cryptographie à University College London (UCL), a, par ailleurs, fait valoir à vos rapporteurs que les cryptomonnaies s'inscrivent dans une **mutation profonde du système des paradis fiscaux** actuel.

Selon lui, leur essor est essentiellement dû à des besoins de contourner les entraves à la liberté de circulation des capitaux. Par exemple en Chine, les flux de capitaux pour les particuliers sont fortement encadrés. Les politiques conduites dans d'autres États conduisent également à restreindre l'exercice de cette liberté (cas de la Russie, Tunisie, Inde, Corée du Sud, etc.).

C. LES PERSPECTIVES EUROPEENNES ET L'IMPASSE DES BLOCKCHAINS SOUVERAINES

Il faut souligner **l'impasse technologique et politique de l'idée théorique des *blockchains* souveraines,** qui ne constituent pas une réponse satisfaisante aux problèmes de souveraineté vus précédemment. En effet, par définition, une *blockchain* publique est un système ouvert, libre de droits et d'utilisation, à vocation universelle, alors qu'une « *blockchain* souveraine » serait fermée, soumise à autorisation d'accès par les autorités publiques.

Vos rapporteurs plaident, en revanche, pour le **développement de *blockchains* européennes** qui, **sans être souveraines**, seraient conçues sur le sol européen, dans le respect de **nos principes politiques, philosophiques et moraux**.

Il est impératif que la recherche et le monde économique investissent dans une technologie qui puisse porter les valeurs européennes, en particulier en termes de développement durable et de protection des données personnelles et du consommateur[2].

L'Union européenne a lancé en 2018 un **observatoire de la *blockchain***. Celui-ci a pour **triple mission** de proposer une approche pédagogique de la technologie à l'attention des citoyens, de constituer un cadre réglementaire pouvant être proposé aux pays membres et, enfin, de réfléchir à des applications qui pourraient faire l'objet de projets européens.

---

[1] http://www.strategie.gouv.fr/publications/enjeux-blockchains

[2] *Le projet BART, vu précédemment, va dans ce sens.*

Vos rapporteurs s'étonnent du choix de la Commission européenne de **recourir à l'entreprise américaine Consensys** pour ce faire. Il s'agit d'une *start-up* d'applications sur Ethereum devenue leader dans ce secteur avec plus de 800 salariés[1]. Joseph Lubin, un des cofondateurs d'Ethereum, ancien cadre dirigeant de Goldman Sachs, a fondé en 2015 cette entreprise qu'il dirige toujours aujourd'hui.

L'Europe devrait **s'emparer de cette question de manière plus stratégique** et éviter la répétition du scénario d'internet. Pour Cyril Grunspan, « *le web était tout de même une invention européenne, qui est passée sous pavillon américain, avec une gouvernance américaine* ».

Les compétences et les domaines de recherche dont la préservation est indispensable pour que la France et l'Union européenne s'approprient la *blockchain* restent encore à préciser, mais il est certain que ce choix de **faire appel à un acteur américain spécialisé dans Ethereum constitue un très mauvais signal**.

Des investissements spécifiques et un effort en matière de recherche paraissent indispensables. Cyril Grunspan rappelle ainsi qu'aux États-Unis « *la blockchain a fait l'objet de cours en ligne dès 2013-2014, dont un, excellent, à l'université de Princeton, écrit par Edward Felten. Le MIT (Massachusetts Institute of Technology) a lancé une initiative sur les monnaies numériques, attirant des stars du secteur comme Gavin Andresen, le développeur à la tête de la Fondation Bitcoin, considéré comme l'héritier de Satoshi Nakamoto* ». De même, au Royaume-Uni, un centre de recherche sur les cryptomonnaies a été ouvert à l'Imperial College de Londres.

D'après le rapport de France Stratégie « *Les Enjeux des blockchains* »[2], les États affichent un intérêt de plus en plus marqué pour ces technologies et des stratégies nationales spécifiques se font jour ici et là : « *après une période où la régulation semblait l'ennemi juré de l'innovation, l'heure semble venue de trouver un moyen de tenir la chaîne par les deux bouts : réglementer de façon coordonnée sur un certain nombre de sujets permettra à la fois de contrôler les usages délictueux et de favoriser les développements souhaités. (…) En réalité, en matière de blockchains, c'est une réponse à l'échelle européenne voire mondiale qu'il conviendrait de viser. (…) Après une période d'expérimentation sans contrainte, il est temps de ''sortir du bac à sable'', selon l'expression usuelle dans l'économie numérique. Par une sorte de convergence naturelle, la plupart des acteurs sont aujourd'hui disposés à entrer dans une nouvelle phase, celle d'une intervention des pouvoirs publics pour fixer un cadre juridique et règlementaire qui permette le plein essor de cette nouvelle technologie* ».

---

[1] *L'entreprise s'est à cet effet associée avec une association suisse et deux universités brittaniques.*

[2] *http://www.strategie.gouv.fr/publications/enjeux-blockchains*

CONCLUSION

Les **perspectives** ouvertes par les *blockchains* sont **considérables** et ne doivent pas être ignorées. C'est pourquoi vos rapporteurs invitent à **prendre au sérieux leurs limites** technologiques et scientifiques actuelles, afin d'encourager la recherche des **solutions les plus pertinentes et les plus pérennes**.

Les principales priorités pour la recherche devraient être la **réduction de la consommation énergétique**, la **capacité** à **monter en charge** (scalabilité), la **sécurité des systèmes** et la **fiabilité des applications**. Il conviendrait également de résoudre la contradiction entre **protection des données personnelles** - qui suppose un certain anonymat - et **lutte contre les fraudes** - qui nécessite une forme de transparence des transactions sur le réseau.

Il convient de s'assurer que **la France et l'Union Européenne se saisissent maintenant pleinement du sujet des *blockchains* en se plaçant à l'avant-garde de leur développement**.

LISTE DES PERSONNES CONSULTEES

M. Gérard Berry, professeur au Collège de France, membre du conseil scientifique de l'Office ;

Mme Emmanuelle Anceaume, chargée de recherche en informatique à l'Institut de recherche en informatique et systèmes aléatoires (Irisa/CNRS/INRIA/IMT Atlantique/ENS Rennes/INSA Rennes/CentraleSupelec/Université de Bretagne Sud/Université de Rennes 1) ;

M. Daniel Augot, directeur de recherche à l'INRIA et à l'École polytechnique ;

Mme Claire Balva, présidente de Blockchain France et de Blockchain Partner ;

M. Billal Chouli, directeur technique de la société NeuroChain ;

M. Nicolas Courtois, professeur d'informatique au University College London (UCL) ;

M. Vincent Danos directeur de recherche au CNRS et à l'École normale supérieure de Paris (ENS Paris) ;

M. Jean-Paul Delahaye, professeur émérite en informatique à l'Université Lille I (Centre de recherche en informatique, signal et automatique de Lille/CRISTAL) ;

M. Gilles Fedak, chargé de recherche à l'INRIA et président d'iExec ;

M. Georg Fuchsbauer, chargé de recherche à l'École normale supérieure de Paris et à l'INRIA ;

Mme Tiphaine Havel, conseillère parlementaire de la CNIL ;

Mme Amandine Jambert, ingénieur expert auprès de la CNIL ;

M. Fabrice Le Fessant, chargé de recherche à l'INRIA et fondateur de OCamlPro, Move&Play et CleverScale ;

M. Renaud Lifchitz, consultant et chercheur en sécurité informatique et en cryptographie ;

M. Gérard Memmi, responsable du département Informatique et Réseaux de Télécom ParisTech ;

M. Ricardo Perez-Marco, directeur de recherche en mathématiques (CNRS/Université Paris Diderot) ;

M. David Pointcheval, directeur de recherche au CNRS, directeur du Département d'Informatique de l'ENS (DIENS), et responsable de l'équipe de cryptographie du DIENS, CNRS-INRIA ;

M. Simon Polrot, avocat, fondateur d'Ethereum France et de VariabL ;

M. Pierre Porthaux, président de Blockchain Solutions et d'EmergenceLab ;

M. Renaud Roquebert, avocat conseil de la société NeuroChain ;

Mme Guilda Rostama, juriste auprès de la CNIL ;

M. Ken Timsit, directeur général de Consensys ;

M. Jérôme de Tychey, directeur du département Solutions (Tech Lead) chez Consensys, chargé de l'observatoire européen de la *blockchain* ;

M. Manuel Valente, directeur de la Maison du Bitcoin ;

M. Jean Zundel, spécialiste d'Ethereum, traducteur du livre blanc sur l'Ethereum de Vitalik Buterin et de la version 2.0 du protocole Ethereum.

BIBLIOGRAPHIE

Ouvrages :

- *Blockchain World*, rapport de l'association mondiale des ingénieurs en électronique (IEEE ou *Institute of Electrical and Electronics Engineers*), 2017, disponible sur ce lien : *https://spectrum.ieee.org/static/special-report-blockchain-world*

- *Blockchain Technology Overview*, National institute of Standards and technology, U.S Department of Commerce, 2018, disponible sur ce lien : *https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf*

- *Blockchain Revolution*, **Don** et **Alex Tapscott**, éditions Penguin Random House, 2016.

- *Global Cryptocurrency Benchmarking Study*, **Garrick Hileman** et **Michel Rauchs**, Université de Cambridge, 2017 disponible sur ce lien : *https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf*

- *Cryptocurrencies : looking beyond the hype*, chapitre du rapport annuel 2018 de la Banque des règlements internationaux, disponible sur ce lien : *https://www.bis.org/publ/arpdf/ar2018e5.pdf*

- *Distributed ledger technology and blockchain*, **H.Natarajan, S.Krause et H.Gradstein**, Banque mondiale, 2017, disponible sur ce lien : *http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain*

- *How Blockchain technologies could change our lives, Science and Technology Options Assessment* (STOA) du service de recherche du Parlement Européen, février 2017, disponible au lien suivant : *http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf*

- *Distributed ledger technology : beyond blockchain*, *United Kingdom Government Office for Science*, 2016, disponible sur ce lien : *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf*

- *Comprendre la Blockchain*, éditions Uchange, 2017, disponible sur ce lien : *https://www.uchange.co/comprendre-la-blockchain/*

- *La Blockchain décryptée – les clefs d'une révolution*, Blockchain France, 2016, disponible sur ce lien : *https://blockchainfrance.net/decouvrir-la-blockchain/la-blockchain-decryptee-les-clefs-dune-revolution/*

- *Les Enjeux des blockchains*, rapport de France Stratégie, 2018, disponible sur ce lien : *http://www.strategie.gouv.fr/publications/enjeux-blockchains*

- *Bitcoin*, **Jacques Favier** et **Adli Takkal Bataille**, CNRS éditions, 2017.

- *Blockchain : la révolution de la confiance*, **Laurent Leloup**, éditions Eyrolles, 2017.

- *Big Bang Blockchain : la seconde révolution d'internet*, **Stéphane Loignon**, éditions Tallandier, 2017.

- *Bitcoin : A Peer-to-Peer Electronic Cash System*, **Satoshi Nakamoto**, disponible sur ce lien : *https://bitcoin.org/bitcoin.pdf* (*traduction en langue française au présent lien*).

- *A Next-Generation Smart Contract and Decentralized Application Platform*, **Vitalik Buterin**, décembre 2013, disponible au lien suivant : *https://github.com/ethereum/wiki/wiki/White-Paper* et en français : *http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/*

- *Mastering Bitcoin : programming the open blockchain*, **Andreas M. Antonopoulos**, éditions O'Reilly, 2017, disponible en français sur ce lien : *https://bitcoin.fr/wp-content/uploads/2016/01/Mastering-Bitcoin.pdf*

- *Bitcoin et Blockchain : vers un nouveau paradigme de la confiance numérique ?*, Revue Banque édition, 2016.

- *Consensus. Immutable agreement for the Internet of value,* Rapport de **Sigrid Seibold et George Samman** pour KPMG disponible au lien suivant : *https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf*

- *Manifeste crypto-anarchiste*, **Tim May,** 1992.

- *Manifeste d'un Cypherpunk*, **Eric Hughes,** 1993.

TA-SWISS, fondation suisse pour l'évaluation des choix technologiques, membre du réseau EPTA dont est également membre l'OPECST, rendra prochainement une étude sur la *blockchain*.

Articles :

Blockchain, Trust machine, *The Economist*, 30 octobre 2015.

Giang-Truong Nguyen et Kyungbaek Kim, « *A survey about consensus algorithms used in blockchain* », dans le « *Journal of Information processing systems* », vol. 14, n° 1, février 2018.

Marc Andreessen, « *Why bitcoin matters* », *New-York Times*, 21 janvier 2014.

Jean-Paul Delahaye, « La folie électrique du Bitcoin », dans « Pour la science », février 2018.

Jérôme Deroulez « Blockchain et données personnelles : quelle protection de la vie privée ? » dans « La Semaine juridique édition générale » n° 38, 18 septembre 2017.

Nina Fabrizi-Racine « La blockchain : (R)évolution d'État ? » dans « La Semaine juridique : Administrations et collectivités territoriales » n° 49, 11 décembre 2017.

Nathalie Devillier « Jouer dans le "bac à sable" réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de blocs » dans « RTD com - revue trimestrielle de droit commercial et de droit économique », n° 4, octobre-décembre 2017.

Morten Bech and Rodney Garratt, « *Central bank cryptocurrencies* », Banque des règlements internationaux, BIS Quarterly Review, septembre 2017.

Les sites suivants peuvent aussi être cités :

www.bitcoin.org

https://bitcoin.info

www.coindesk.com

https://cointelegraph.com

https://blockchain.info

https://bitnodes.earn.com

https://bitinfocharts.com

https://statoshi.info

https://bitcoinchain.com/pools

https://digiconomist.net

https://blockchainfrance.net

https://blockchainpartner.fr

et https://journalducoin.com

SYNTHESES DES AUDITIONS CONDUITES PAR LES RAPPORTEURS

I. AUDITIONS DU 27 MARS 2018

1. Mme Claire Balva, présidente de Blockchain Partner

Claire Balva est diplômée de l'ESCP-Europe (École Supérieure de Commerce de Paris) et a découvert le « monde de la *blockchain* » en 2014, après quelques expériences professionnelles dans le développement d'affaires et le marketing. Avec trois anciens étudiants de l'ESCP, elle fonde Blockchain France, puis Blockchain Partner, dont elle est la dirigeante exécutive.

Blockchain Partner est une société qui propose trois activités autour des protocoles de chaînes de blocs : de la formation, du conseil stratégique et du développement technique. Leurs principaux clients sont de grandes entreprises et institutions. Parmi leurs derniers projets en date figure une coopération avec la Banque de France ou la publication d'un guide sur les enjeux juridique des chaînes de blocs. Blockchain France continue cependant d'exister.

Le bitcoin

Claire Balva débute sa présentation par un historique du bitcoin, s'agissant de la première apparition d'une *blockchain* telle qu'on l'entend aujourd'hui. **En 2008, dans un livre blanc publié par un ou plusieurs anonymes signant sous le pseudonyme de Satoshi Nakamoto, ce protocole informatique propose la création d'une monnaie électronique fonctionnant sur un système pair à pair.**

Elle rappelle que sur internet, toute donnée est facilement copiable à l'infini, ce qui conditionnait jusque-là la création d'une monnaie purement électronique à l'existence d'un intermédiaire qui centralise les transactions. **Avec le bitcoin, l'intermédiaire existe toujours, mais il est décentralisé : c'est la *blockchain*, un registre de transaction évolutif**. N'importe qui peut télécharger cette *blockchain* et la tenir à jour en ajoutant au fur et à mesure des blocs comprenant des transactions. Ces blocs sont créés toutes les dix minutes.

Longtemps très confidentiel et valant quelques dollars, le bitcoin a vu son cours augmenter considérablement avec un premier pic en 2013 à plus de 1 000 $, largement effacé par le pic actuel (20 000 $ fin 2017) ; il est aujourd'hui autour de 8 000 $. Le site blockchain.info permet de suivre son évolution.

Malgré sa forte valeur, le bitcoin est divisible jusqu'à 10^{-8}, ce qui permet de financer des petites transactions, la plus petite unité étant appelée satoshi.

Concrètement, pour vendre et acheter des bitcoins il existe des plateformes, dont la plus connue est Coinbase.

Posséder des bitcoins revient à posséder une clé privée, c'est-à-dire un code unique et impossible à recréer par un tiers, donnant accès aux transactions reçues. Un propriétaire de bitcoin peut soit déléguer le stockage de ses clés à une plateforme en ligne, soit conserver personnellement ses codes sur n'importe quel support physique. Cette clé seule donnant accès aux bitcoins, **si la plateforme est piratée ou si l'on égare son support physique, il n'est plus possible de récupérer les crypto-actifs stockés**.

Le protocole Bitcoin prévoit une création échelonnée des bitcoins, décroissante dans le temps, qui sera limitée au final à 21 millions d'unités, ce qui n'est pas le cas de tous les crypto-actifs.

Ronan Le Gleut s'interroge sur la viabilité du système Bitcoin. N'est-il pas condamné à exploser, les blocks étant limités à un méga et les transactions augmentant indéfiniment ?

Pour Claire Balva, la scalabilité est effectivement un problème pour le développement futur du bitcoin. **La scalabilité représente le nombre de transactions pouvant passer sur le réseau en même temps**. Celui-ci étant souvent sur-sollicité, il y a des transactions en attente. Pour prioriser une transaction, il faut alors payer plus de frais de transaction, ceux-ci ont pu s'élever jusqu'à 20 € lors des pics les plus importants, contre quelques dixièmes de centimes en temps normal.

Toutefois, Claire Balva fait remarquer que les capacités de stockage ont tendance à augmenter de manière exponentielle là où les besoins de stockage dans la *blockchain* augmentent de manière linéaire, le rythme d'ajout de nouveaux blocs étant régulier. **On peut donc estimer, selon elle, que les capacités de stockage seront longtemps suffisantes pour soutenir la croissance du poids de la *blockchain***. Sur blockchain.info, il est possible de suivre l'évolution du poids en mégabits de la *blockchain* du bitcoin.

D'autre part, le protocole Bitcoin a déjà pu connaître des évolutions pour répondre à ces enjeux de scalabilité, une mise à jour a ainsi permis d'augmenter le nombre de transactions stockables dans un même bloc.

Définition et fonctionnement de la blockchain

Claire Balva présente ensuite le fonctionnement de la *blockchain*. Selon elle, il s'agit d'**une base de données structurée en blocs regroupant des données, comme des transactions**, mais pas uniquement. **Elle est immuable, c'est-à-dire que de nouveaux blocs s'ajoutent constamment, chacun de ces blocs étant horodaté lors de sa validation par le mineur qui l'a obtenu. Chacun de ces blocs et des données qu'il contient sont ensuite envoyés à l'ensemble des nœuds du réseau par un système de pair à pair**, c'est-à-dire que le premier nœud à posséder le bloc l'envoie à plusieurs autres nœuds qui lui sont connectés, ceux-ci reproduisant le même mécanisme.

Le **hashage** est une fonction mathématique utilisée à plusieurs étapes d'un protocole de *blockchain*. Sur les grandes *blockchains*, la fonction de hashage utilisable est SHA-256. À partir d'un grand ensemble de données, elle va créer une chaîne unique de 256 bits, tout changement même mineur sur l'ensemble de données de départ donnera lieu à une chaîne totalement différente.

Ces caractéristiques permettent :

- de vérifier l'intégrité d'un document ;

- de « signer » un document sans en révéler le contenu, c'est-à-dire de prouver sa possession ;

- répétées plusieurs fois, d'obliger un ordinateur à utiliser une grande puissance de calcul.

Claire Balva fait la démonstration d'un hashage sur anders.com/blockchain/hash.html

Elle présente ensuite la composition d'une chaîne de blocs. L'identifiant d'un bloc donné est le hash de ce bloc, qui sera copié dans le bloc suivant. C'est ainsi que **les blocs sont tous liés entre eux cryptographiquement**. En effet, si on tente de modifier les données d'un bloc, son hash change, et le hash du bloc suivant aussi. Il faudrait donc au hacker recalculer l'ensemble des blocs suivant celui qu'il a modifié.

Elle en fait la démonstration sur :

anders.com/blockchain/blockchain.html

Pour rendre cela trop coûteux et donc impossible, l'ajout d'un nouveau bloc est conditionné à un processus appelé minage.

Le minage

La plupart du temps, **ce minage consiste en la résolution d'une épreuve cryptographique, appelée preuve de travail** (*proof of work*). Il s'agit de calculer le hash de ce bloc en y ajoutant un « nonce », c'est-à-dire quelques chiffres, avec lequel le hash obtenu répond à une certaine propriété, par exemple qu'il commence par un certain nombre de 0.

Le seul moyen d'obtenir ce résultat est de tester plusieurs nonces, jusqu'à trouver le bon, sans que rien n'indique si le mineur est proche ou non de trouver le bon nonce. En exigeant un certain nombre de 0 en début de hash, la probabilité de trouver le nonce correct peut baisser très rapidement jusqu'à devenir infime. Il faut alors réaliser un très grand nombre de calculs pour avoir une chance de le trouver, ce qui a un coût énergétique et temporel (en moyenne 10 minutes, dans le cas du bitcoin).

Les mineurs vont néanmoins opérer ces calculs parce qu'ils y trouvent un double intérêt : ils peuvent **toucher les frais de chaque transaction** qu'ils intègrent dans leur bloc, et obtenir **une récompense en crypto-actifs** attribuée par le protocole lorsqu'ils trouvent un bloc.

Les mineurs sont en concurrence car seul celui qui trouve le bloc obtient la récompense. C'est cette compétition colossale qui fait la sécurité du réseau car **il est très difficile pour une seule entité de miner plus vite que toutes les autres réunies** et donc de recalculer toute une chaîne de bloc plus rapidement que la chaîne principale qui continue de se construire.

Le bitcoin voit toutefois aujourd'hui son minage concentré dans de grandes fermes ou dans des *pools* (regroupement de mineurs), dont cinq possèderaient aujourd'hui la moitié de la puissance de calcul totale. **Lorsque les mineurs sont trop**

concentrés, cela envoie un mauvais signal au reste du réseau car il perd de sa décentralisation.

Toutefois, **les mineurs ont tendance à s'autoréguler et à se diviser d'eux-mêmes lorsqu'ils deviennent trop concentrés**. En effet, ils ont tout intérêt à conserver la confiance des utilisateurs dans le réseau, en cas de doute ceux-ci cesseront en effet d'utiliser la *blockchain*. Ceci ferait baisser la valeur des crypto-actifs qu'ils reçoivent en récompense de leur travail.

Si la puissance augmente sur le réseau de telle manière à ce qu'un bloc ne soit plus créé toutes les 10 minutes mais dans un temps plus court, celui-ci se réadapte tout seul en augmentant la difficulté de la fonction de hashage (c'est-à-dire en augmentant le nombre de 0 à trouver).

Il est évident que la preuve de travail consomme beaucoup d'énergie mais il est complexe d'en faire une estimation quantitative.

Blockchains publiques et privées

Il y a différents types de *blockchains*, on distingue souvent *blockchains* publiques et privées. **Bitcoin** est une ***blockchain* publique** (*permissionless)* c'est-à-dire ouverte à tous, lisible par tous et à laquelle n'importe qui peut ajouter un bloc (sous réserve de l'avoir miné).

A l'inverse, les solutions comme ***Hypeldeger*** sont des ***blockchains* privées** (*permissioned)*, l'accès y est limité par une autorité centrale qui en contrôle plus ou moins le fonctionnement.

D'autres solutions comme **Ethereum** se situent à un niveau plus intermédiaire, l'accès étant libre, mais une équipe connue de développeurs travaillent sur le code. Le principal intérêt d'Ethereum est de pouvoir inscrire de courts programmes sur la *blockchain*, les « *smart contracts* ». Selon Claire Balva, **« *s'il y a une figure à retenir aujourd'hui dans le monde de la blockchain, c'est Vitalik Buterin* »,** son inventeur.

Le bitcoin reste l'actif dominant sur le marché avec près de 50 % de la capitalisation totale des crypto-actifs. Toutefois, cette part a tendance à se réduire au profit d'une multitude d'autres crypto-actifs. Ses concurrents les plus importants à ce jour sont Ethereum, Ripple, Bitcoin Cash et Litecoin.

Autres modes de preuve

Une seconde distinction entre *blockchains* touche à **la méthode de consensus**, plusieurs modèles alternatifs à la *proof of work* existent en effet. Claire Balva en présente deux :

La **preuve d'enjeu** (*proof of stake*) consiste pour les mineurs à prouver la possession d'une certaine quantité de crypto-actifs pour avoir l'opportunité de « forger » un bloc et d'y intégrer des transactions. C'est le système adopté entre autres par *NXT*, depuis deux ans Ethereum annonce vouloir y passer.

Toutefois, c'est d'une part un système très capitalistique où avoir plus de jetons donne plus de chances d'être validé, d'autre part la technique est encore très expérimentale et sa fiabilité par rapport à la preuve de travail n'est pas démontrée.

La **preuve d'autorité** (*proof of authority*) est propre aux protocoles privés. C'est le mode de consensus le plus simple. Une autorité centrale attribue le droit de miner un bloc selon des modalités définies par elle. Cela correspond à centraliser partiellement le réseau.

Couches techniques

Selon Claire Balva, **les protocoles de *blockchain* devraient être placés entre la couche technique correspondant à TCP/IP et une couche applicative** (*tokens, Dapps*…), qui supporte finalement les interfaces client. En effet, la *blockchain* peut avoir d'autres types d'application que les transactions et le transfert d'actifs.

Elle peut ainsi servir de registre certifiant, pour enregistrer l'empreinte cryptographique (hash) d'un document et permettre ainsi de prouver l'existence d'un document à moment T.

Smart contract

Une autre application est le « ***smart contract*** », **un court programme exécutable stocké comme une transaction**. Utiliser la clé publique de cette transaction permet alors de déclencher l'exécution de ce programme, si certaines conditions sont respectées.

Ainsi l'assureur Axa a-t-il pu programmer un remboursement automatique en cas de retard d'un vol d'avion. **L'oracle joue ici un rôle crucial, il s'agit d'un tiers qui récupère des données externes et les envoie dans la *blockchain***, ce qui pourra éventuellement déclencher l'exécution d'un contrat. Selon Claire Balva un tel système a toutefois un avantage comparatif limité par rapport à d'autres systèmes existants, pour une compagnie bénéficiant déjà de sa propre infrastructure bancaire. En revanche, il peut être très utile à une start-up qui pourra s'exonérer d'un intermédiaire bancaire ou assurantiel.

Un autre exemple de *smart contract* a été développé par Blockchain Partner avec la Banque de France et ses partenaires, pour la gestion de documents SEPA.

ICO

Les ***Initial Coin Offering*** sont des levées de fond spécifiques à l'écosystème *blockchain*, où **le financement se fait par échange de cryptomonnaies contre des *tokens***. Ces *tokens*, spécifiques au projet financé, sont des jetons inscrits sur la *blockchain* qui peuvent donner accès à des droits ou à des services. Ce système se différencie du *crowdfunding* en ce que les contreparties (*tokens*) peuvent être échangées sur un marché secondaire où elles ont un cours.

Ces ICO permettent à des start-ups accédant difficilement à des financements classiques de réaliser de très importantes levées de fond, pouvant dépasser la centaine de millions de dollars. Aujourd'hui, les ICO se font souvent moins en bitcoin qu'en ether, ceux-ci permettant le reversement automatique de la contrepartie grâce à des *smarts contracts*.

2. M. Renaud Lifchitz, consultant et chercheur en sécurité informatique

Renaud Lifchitz est ingénieur en informatique, il fut le premier à faire une conférence publique en France sur le bitcoin, en juin 2011. Il a mené de nombreuses recherches sur la *blockchain*, mais aussi entre autres sur les failles de sécurité du paiement sans contact.

Il a été mentionné en 2014 par le ministère de l'économie numérique comme l'un des 100 experts mondiaux en technologies de l'information. Récemment, il a obtenu deux « certifications *blockchain* » du Blockchain Council.

Définition de la blockchain

Pour Renaud Lifchitz, **la *blockchain* est un réseau global distribué sans aucun point unique de défaillance qui permet la transmission d'informations authentifiées, fiables et sûres, et qui présente de multiples usages**.

À la demande des parlementaires, il fait un rappel du fonctionnement de la technologie. Il indique notamment qu'une transaction ne met en moyenne que cinq secondes à être propagée sur l'ensemble du globe, ce sont les opérations d'intégration dans un bloc et de validation qui prennent du temps. Les transactions envoyées patientent en file d'attente jusqu'à pouvoir être intégrées dans un bloc.

Il arrive que des blocs vides soient produits, y compris encore aujourd'hui sur Bitcoin. Il reste toutefois plus intéressant pour un mineur d'inclure des transactions pour en toucher les frais.

Il apporte des précisions concernant les nœuds :

- **est un nœud toute personne qui a téléchargé la *blockchain* et qui la met à jour**. La plupart des utilisateurs *lambda* n'ont pas de nœud en propre. En effet, gérer un nœud suppose d'avoir suffisamment de capacité de stockage. En pratique, la plupart des utilisateurs se connectent donc à un nœud pour effectuer leurs transactions, sans en posséder en propre ;

- **la plupart des nœuds sont des mineurs, on parle de nœuds actifs**. Historiquement, tous les mineurs détenaient le registre, désormais ce n'est plus toujours le cas ;

- **d'autres nœuds servent seulement à surveiller la *blockchain* ou à y donner accès, on parle alors de nœuds passifs**. Ils vont tout de même avoir un rôle de relais, après vérification de la validité des blocs qui leurs sont envoyés.

Il ne faut pas confondre la vérification de la validité avec celle de la véracité des transactions, qui est plutôt effectuée par le récipiendaire final.

Sur Bitcoin, on dénombre entre 8 000 et 15 000 nœuds. Le choix du nœud auquel un utilisateur se connecte est laissé à son appréciation, ou à celle de l'éditeur du logiciel qu'il utilise pour effectuer ses transactions.

Cinématique d'une transaction sur la blockchain

Trois outils cryptographiques sont utilisés dans le protocole *blockchain* :

- le chiffrement asymétrique pour la signature électronique et la communication sécurisée entre deux points ;

- le chiffrement symétrique pour la communication sécurisée entre deux points ;

- les fonctions de hachage.

Lorsqu'un utilisateur souhaite effectuer une transaction *blockchain* : il choisit depuis quels comptes il souhaite faire des débits et vers quel compte il fait le crédit.

1 - Les informations essentielles de la transaction (adresses d'entrées et sorties, montants) sont **hachées électroniquement**.

2 - La transaction est ensuite **signée électroniquement**.

3 - La transaction est envoyée aux voisins sur le réseau.

4 - Les voisins vérifient que les fonds sont disponibles et que la/les **signatures sont valides** avant de relayer la transaction.

5 - La transaction est placée avec d'autres dans une file d'attente avant qu'elles soient **regroupées dans un bloc**.

6 - Un mineur «scelle» plusieurs transactions **en les ordonnant dans un bloc, en calculant une empreinte de ce bloc**, **et en le diffusant à ses voisins**.

7 - Le scellement nécessite la résolution d'un problème complexe basé sur les **fonctions de hachage**, **ce problème permet implicitement de créer de la confiance entre nœuds du réseau qui ne se connaissent pas**.

Intérêts de la blockchain

- **La scalabilité** liée à la facilité pour déployer des nœuds. Il y a un engorgement mais malgré tout sur Bitcoin, 50 % des transactions passent en moins de deux blocs, ce qui reste relativement rapide.

- **La résilience**, c'est-à-dire la capacité de résistance aux attaques de tout type (réseau, applicatives, dénis de service…). La seule attaque sérieusement dangereuse est celle des 51 %.

- **L'intégrité et l'authenticité des données**, quand on signe et scelle une transaction, on sait à qui et quand elle a été faite, de manière certaine. « *Toutes les transactions sont signées, ce qui ne signifie pas que ce n'est pas anonyme, on parle de transactions pseudonymes* ».

- **La décentralisation**, il n'existe pas de point de défaillance unique et il n'est plus besoin de tiers de confiance.

- **La rapidité** des transactions par rapport aux réseaux interbancaires (ex : *SWIFT*). Pour améliorer la rapidité, des améliorations sont possibles. La

mise à jour ayant permis le réagencement des transactions dans les blocs Bitcoin a été appelée **segwit**.

Technologies de registres distribués

Les *blockchains* sont une sous-catégorie de la famille des *distributed ledger technologies* (DLT), qui comprend notamment HashGraph, Tangle/DAG (Directed Acylcic Graph)… Ces derniers n'ont pas de chaîne unique structurée par des blocs mais présentent un profil de transactions validées une par une. À l'heure actuelle, la sécurité de ces technologies alternatives n'est toutefois pas prouvée.

Satoshi Nakamoto

Selon Renaud Lipchitz, derrière Sakoshi Nakamoto se cacherait un groupe de cinq à six personnes de compétences complémentaires. À ce sujet, il conseille un podcast de Jean-Jacques Quisquater[1], l'un des seuls chercheurs à être cité par Nakamoto.

Usages

« *Il ne faudrait surtout pas considérer qu'une blockchain est uniquement un réseau financier* ». Cela dit, de nombreux cas d'usage ne justifient pas l'usage d'une *blockchain* :

- les transactions sont très **limitées en taille et en nombre** (Bitcoin est limité à 3-7 transactions par seconde, Ethereum entre 7 et 15) ;

- le système est **coûteux énergétiquement** parlant (par rapport à une redondance informatique classique) ;

- le **stockage de données brutes est coûteux et public**. Cela pose un gros problème avec le RGPD, notamment en termes de respect du droit à l'oubli, car tout est en clair et tout est archivé. En effet, chiffrer des données coûte cher et prend du temps. Une parade consiste à ne stocker que l'identifiant ou le hash d'un ensemble de données dans la *blockchain*, mais ce n'est utile que dans certains cas.

Plusieurs facteurs favorisent et légitiment par contre l'adoption d'une *blockchain* :

- **en cas d'absence de confiance a priori** entre participants « *le grand intérêt de la blockchain c'est de créer un réseau de confiance en ne connaissant personne dans celui-ci* » ;

[1] https://www.nolimitsecu.fr/interview-de-jean-jacques-quisquater/

- si l'on souhaite une écriture par des acteurs indépendants tout en réduisant les coûts classiquement associés à cette indépendance (temporels et financiers) ;

- dans tous les cas où l'on recherche de la **désintermédiation.**

Exemples d'usages : en Estonie, 99 % des prestations de l'État se font en ligne, à distance. Pour ouvrir une société, un compte en banque, voter… Afin d'identifier les citoyens, on utilise leur signature électronique qui est stockée sur une *blockchain*. Au Sierra Leone, la *blockchain* est utilisée pour le vote électronique, mais aussi en France dans une petite commune qui organise des « référendums flashs ».

D'autres grands domaines d'usage seront la banque, l'assurance, le notariat, la conservation de la preuve, la collecte ou encore l'exécution conditionnelle de transactions (*smart contract*).

Bonnes pratiques de sécurité

Pour garantir la sécurité des réseaux, il faut se concentrer sur trois axes relativement simples :

- **avoir des algorithmes de cryptage à jour**, car la cryptographie évolue et devient de plus en plus puissante ;

- **inventer des mots de passe complexes** utilisant plusieurs caractères, chiffres et des caractères spéciaux ;

- **faire un bon usage des modes de blocs**, c'est-à-dire prévoir que le chiffrage évolue afin d'éviter que l'on ne puisse retrouver des motifs récurrents (ex : cassage de la machine Enigma II, durant la seconde guerre mondiale).

Du point de vue de la sécurité, une *blockchain* comme celle du bitcoin est aujourd'hui largement au-dessus de ce que suggèrent les référentiels RGS (ANSSI) en France, ou NIST et SOX aux États-Unis.

Démocratie et évolution d'une blockchain

Des développeurs peuvent proposer des améliorations sur une *blockchain*, mais elle ne sera réellement effective que si elle est adoptée largement dans le réseau. Le « vote » se fait finalement en acceptant ou refusant une mise à jour.

Selon les communautés et les *blockchains*, on observera une approche variable du compromis entre sécurité et flexibilité. La communauté du bitcoin est la plus conservatrice, la sécurité y est nettement considérée comme l'enjeu le plus important.

Parfois se créent des *hard forks*, c'est-à-dire que toute une partie du réseau s'émancipe autour d'une nouvelle *blockchain*. Ce fut le cas de Bitcoin Cash par exemple, un projet annexe permettant une plus grande fluidité d'échanges. Le projet principal, Bitcoin Core, reste toutefois largement majoritaire.

3. M. Ricardo Perez-Marco, directeur de recherche en mathématiques

Ricardo Perez-Marco a découvert la *blockchain* via le bitcoin, en lisant le papier de Satoshi Nakamoto qu'il a trouvé sérieux. Pour lui, il s'agit d'un **réseau automatique qui crée de la confiance entre personnes qui ne peuvent pas se faire confiance.** Beaucoup d'experts auto-proclamés essaient de vendre leur *blockchain*, mais selon lui l'état de l'art est plus complexe que ce qu'ils présentent.

Le bitcoin : l'or électronique

L'idée du créateur est de créer de la rareté (comme pour l'or), avec une masse monétaire programmée. Cela a beaucoup heurté les économistes classiques qui sont convaincus qu'une monnaie déflationniste ne peut pas fonctionner, or le bitcoin est déflationniste par nature.

Tous les quatre ans le nombre de bitcoins offerts en récompense aux mineurs est divisé par deux, cela s'appelle un *halving* (réduction de moitié), le prochain aura lieu en 2020.

Sur les autres blockchains

Pour Ricardo Perez-Marco, des *blockchains* « privées » comme R3 (consortium bancaire) ne peuvent pas être qualifiées de *blockchain*. En tout cas ce ne sont pas des innovations, les bases de données partagées existaient en effet déjà auparavant. Il est absolument nécessaire que les transactions soient publiques pour qu'un système décentralisé fonctionne.

Selon lui, **la *proof of stake* n'est pas prouvée mathématiquement et n'est donc pas sûre**. La *proof of work* seule permet de se prémunir de façon sûre des **attaques sybil**, c'est-à-dire de la multiplication de nœuds détenus par un seul utilisateur pour dominer le réseau. Cette protection par la preuve de travail existait déjà pour lutter contre les pourriels, entre autres.

On pourrait comparer la *blockchain* privée à un intranet et la *blockchain* publique à internet. Ce sont deux technologies utiles dans leurs champs d'application respectifs mais elles restent indéniablement différentes.

Selon lui, les usages qui vont vraiment progresser sont les plus simples. Par exemple, la *blockchain* permet de prouver la possession d'un document à un moment donné, « ***c'est la première fois qu'on a un serveur de temps universel*** ».

Concernant les usages non financiers, « *ce qui fait qu'il est difficile d'intégrer un projet blockchain pour toutes les applications c'est qu'il faut trouver une incitation indépendante du réseau* ».

Ordinateur quantique

Un ordinateur quantique n'est pas un ordinateur plus rapide mais un système qui donne une réponse immédiate à une équation donnée, mais il ne concerne pas toutes les équations. Cependant, **le cas échéant, certains algorithmes tomberont**

(notamment les asymétriques qui servent à la signature), mais pas les algorithmes de hash. Il faudrait donc réviser le réseau, mais pas le reconstruire entièrement.

Selon Ricardo Perez-Marco, toutefois, l'ordinateur quantique est encore aujourd'hui de l'ordre de la science-fiction.

Réseau de confiance et problème des généraux byzantins

Le problème des généraux byzantins se pose en ces termes : « ***Comment atteindre le consensus dans un réseau où les communications ne sont pas sécurisées et où il existe des nœuds corrompus, mais une majorité d'agents honnêtes ?*** ».

La grande différence entre le problème général et celui de Nakamoto réside dans le fait que les généraux ne soient pas connus dans le second. Par ailleurs, dans le problème général, l'objectif est de coordonner l'action pour effectuer une attaque, dans l'autre il s'agit d'éviter une double dépense en validant collectivement les transactions.

La solution à ce problème dans le bitcoin consiste à choisir au hasard qui validera la prochaine transaction, comme dans une loterie. Mais pour éviter qu'une même entité emprunte plusieurs identités (attaque Sybil), on exige une preuve de travail.

Dans une preuve de travail, le problème est difficile à résoudre mais la solution très rapide à vérifier, **le problème est réajusté tous les 1 000 blocs environ** pour rester autour d'une moyenne de 10 minutes par bloc.

Pour que les mineurs soient incités à investir de la puissance de calcul, on leur attribue une récompense en bitcoin.

Lorsqu'un bloc est forgé, il y a encore un risque qu'un second soit créé avec un hash valide et que quelqu'un puisse pratiquer une double dépense (*double spend*). Pour avoir une certitude totale, il est conseillé d'attendre la confirmation de six autres blocs.

L'énergie produite pour finalement ne pas obtenir un hash correct paraît considérable, dès lors qu'il n'y a qu'un seul gagnant. Mais **on ne peut pas dire qu'elle est inutile** puisque de cette quantité d'énergie dépend la sécurité du réseau. **Plus il y a d'énergie investie sur l'ensemble du réseau, plus il est difficile pour une seule entité de posséder 51 % de la puissance de calcul**.

Génération des adresses

Les adresses sont générées aléatoirement en 256 bits. Il n'y a donc pas de registre d'adresses, mais la loi des grands nombres fait qu'il est hautement improbable, voire impossible à l'échelle du réseau, que deux comptes aient la même adresse (une chance sur 2^{256}).

Ces adresses correspondent à une clé publique vers laquelle on peut effectuer un versement, et à une clé privée qui sert à valider la dépense d'une transaction.

Le point fondamental de la sécurité du bitcoin est de protéger ses clés privées. Si l'on perd sa clé, on perd aussi la transaction qui y est liée. Il y aurait d'ailleurs au moins un quart des bitcoins perdus, cette valeur étant toutefois difficile à estimer. Il y a un enjeu de confiance à ce que les bitcoiners ne permettent pas que ces sommes soient

« récupérées » par une modification du code, c'est une garantie de la fiabilité du bitcoin.

Récompense des mineurs et halving

Au départ, les mineurs recevaient cinquante bitcoins. **Cette récompense est divisée par deux tous les 210 000 blocs** (ce qui correspond environ à quatre ans). Jusqu'en 2016 ils étaient récompensés de 25 BTC, puis jusqu'en 2020 ils le seront de 12,5 BTC.

Le bitcoin n'atteindra donc jamais sa limite asymptotique à 21 millions. Les *halvings* continueront toutefois longtemps car **chaque bitcoin peut être divisé en 100 millions de satoshis**.

De l'argent programmable

Le bitcoin peut être qualifié d'**argent programmable**, car en plus des transactions, de la place est disponible pour insérer quelques lignes de code exécutable. Cela permet notamment de créer des **couloirs de paiement** ou de ne transmettre les fonds à une adresse que si un ou plusieurs tiers utilisent leurs clés privées (*multisig*).

Dans Bitcoin Core cependant, cette possibilité d'écrire des scripts a été limitée car elle entraînait des bugs.

Pour tester ces contrats ou des modifications du code de base, il existe un réseau parallèle appelé *TestNet* qui sert de « bac à sable ». De manière générale, dans le bitcoin, les utilisateurs ne veulent pas changer le code de façon trop radicale pour ne pas prendre le risque de faire tomber tout le réseau.

Fiabilité des autres blockchains

Contrairement à d'autres *blockchains*, le papier originel du bitcoin a été écrit par des scientifiques reconnus. Parmi eux ou parmi ses premiers relecteurs, il y avait notamment **Hal Finney**, cryptographe réputé et développeur des premiers systèmes *pretty good privacy* (PGP) à clé publique délivrés sur le marché.

En ce qui concerne Ethereum, de gros doutes persistent sur sa dimension décentralisée, notamment en raison de la création par le passé d'une hard fork, c'est-à-dire d'une remise à zéro de branches entières du réseau.

Selon Ricardo Perez-Marco, il y a un effet de mode, « ***95 % des monnaies créées aujourd'hui vont disparaître*** ». La technologie *blockchain* va plutôt se développer sur les projets purement décentralisés. Parmi les usages non-transactionnels possibles il imagine :

- une loterie internationale ;
- des services de notariat ;
- un suivi de l'argent public.

II. AUDITIONS DU 28 MARS 2018

1. Mme Emmanuelle Anceaume, chargée de recherche en informatique (IRISA-CNRS)

Emmanuelle Anceaume rappelle que la *blockchain* est très fortement liée au bitcoin, qu'elle qualifie de « ***monnaie virtuelle qui ne repose sur aucune entité de confiance ou de contrôle*** », dont toutes les transactions sont stockées dans un registre public (*public ledger*) que chacun peut auditer pour en vérifier l'intégrité.

Différents types d'utilisateurs

- un utilisateur peut faire des transactions et n'avoir pas téléchargé le client bitcoin, il n'est pas nœud du système ;

- un utilisateur peut faire des transactions et avoir téléchargé le client bitcoin, il est nœud du système et peut ne pas vérifier systématiquement la validité de la *blockchain* ;

- un utilisateur peut faire des transactions et avoir téléchargé le client bitcoin, être donc nœud du système et vérifier systématiquement la validité de la *blockchain* ;

- un utilisateur peut être mineur, et tenter de résoudre les algorithmes de hash pour obtenir des blocs à ajouter au système.

Pour être tout à fait certain que ses transactions sont effectuées, un utilisateur devrait vérifier la validité de la *blockchain* en tout temps (à chaque ajout de bloc).

Transactions

Toutes les transactions qui ont été créées depuis 2009 doivent être conservées dans la *blockchain*, elles y restent *ad vitam aeternam*.

Concrètement, dans une transaction sur le réseau Bitcoin il est inscrit :

- le compte d'Alice (*input address*), c'est-à-dire l'adresse Bitcoin d'Alice et les codes des satoshis qu'elle envoie ;

- le compte de Bob (*output address*), c'est-à-dire la clé publique de Bob et les satoshis qu'il reçoit ;

- les frais de transaction, c'est-à-dire les satoshis qui seront donnés au mineur du bloc dans lequel sera intégrée la transaction.

Ceci signifie notamment que l'*output* est toujours plus petit que l'*input,* puisqu'on lui soustrait les frais de transaction. **Un compte est toujours entièrement débité lorsqu'il est mis en entrée d'une transaction, c'est donc un « objet cryptographique » à usage unique**.

Dans le bitcoin on veut juste savoir qu'une entité qui a créé un compte est bien la seule à avoir pu fournir une transaction, pour conserver la confiance dans le système, c'est pour cela qu'on utilise **une clé publique** que chacun peut vérifier.

A l'inverse, il n'y a qu'une seule personne qui peut recevoir la transaction, celle qui possède **la clé privée** de l'adresse de réception (qui est une clé publique). Il est conseillé de créer un nouveau compte de réception (*output address*) pour chaque transaction que l'on fait, par souci de confidentialité. **Il n'est en effet pas compliqué de créer une paire clé privée-clé**

publique, il est possible d'en créer une infinité sans avoir besoin de les faire enregistrer par une entité tierce.

Un **portefeuille de clés privés** (*wallet*) référence toutes les clés privées d'un utilisateur et les clés publiques auxquelles elles réfèrent, c'est-à-dire tous ses comptes. En d'autres termes, cela lui permet d'accéder à toutes ses transactions reçues, pour éventuellement les dépenser en les envoyant vers une autre adresse de réception.

Sur chaque compte est inscrite la preuve de possession du satoshi précédent, c'est-à-dire qu'il réfère à la transaction précédente. Cette preuve consiste en une signature électronique de la transaction précédente. **De transaction en transaction il est possible de remonter à l'origine de la création du satoshi et donc de vérifier qu'il n'y a pas de double dépense.**

Vérifications

Pour faire effectuer les différentes étapes de vérification, le bitcoin utilise un langage de script très simple, qui s'appelle justement *Script*. C'est un langage **à pile**, on entasse les instructions dans un ordre donné, puis le récepteur les exécutera dans l'ordre inverse.

Lorsque *Bob* reçoit une transaction, il va exécuter ces instructions. C'est-à-dire copier la clé publique, puis réaliser son hash à deux reprises et vérifier qu'elle est conforme. Si c'est le cas, cela signifie que les satoshis envoyés correspondent bien à l'émetteur, on marquera alors le compte émetteur comme vide, et le compte récepteur comme plein.

Cela rend la double dépense impossible : **une fois qu'un compte est marqué quelque part sur la *blockchain* comme vide, il ne pourra plus jamais être utilisé**.

Preuve de travail et minage

Elle a un triple intérêt pour le bon fonctionnement du protocole :

- **limiter l'apparition sur le réseau de deux blocs concurrents au même moment** ;

- donner au bitcoin les caractéristiques d'une monnaie **en garantissant sa rareté et la stabilité de son émission** ;

- **se prémunir des attaques Sybil**.

Emmanuelle Anceaume décrit ensuite les modalités de la preuve de travail. Elle explique notamment que chercher un certain nombre de 0 en début de hash revient à faire **une inversion partielle** du hash. Une fonction de hashage ou un algorithme de chiffrement sont des **primitives cryptographiques**.

Si l'on crée un bloc qui est valide, les mineurs vont se mettre à travailler dessus. Toutefois, ce n'est pas parce qu'on a obtenu un bloc qui est valide que l'on reçoit ses 12,5 bitcoins, **il faut qu'il y ait 100 blocs en plus** pour que la transaction soit validée.

Il arrive que deux blocs soient créés concomitamment. Les mineurs vont alors partir sur la branche la plus longue, ou **plus précisément sur celle qui a demandé le plus de travail**. À partir du moment où un adversaire ne bénéficie pas de plus de 51 % de la puissance de calcul, personne ne peut espérer construire une chaîne sur un autre bloc plus rapidement.

Un **arbre de Merkle** est le nom donné à une suite de blocs de données qui comportent chacun le hash du bloc précédent. Le dernier hash est appelé **racine de Merkle** (*Merkle root*). Le bloc originel, au début de la *blockchain*, est appelé **bloc de Genèse** (*Genesis block*).

La preuve d'enjeu consomme moins d'énergie mais demande de prendre en compte très finement la dynamique des échanges si l'on veut éviter une dérive capitalistique.

Distinctions publiques/privées

Emmanuelle Anceaume distingue trois catégories de *blockchains* :

- la *blockchain* publique (permissionless) est ouverte à tout le monde, lisible par tous ;

- la ***blockchain* de consortium,** qui n'est pas ouverte, seules certaines entités ont le droit de lire et d'écrire. Puisqu'elles se connaissent, elles n'ont pas besoin de preuve de travail ;

- la *blockchain* fermée (permissioned) est maintenue par une entité identifiée. **Pour Emmanuelle Anceaume, ce principe de chaîne de blocs existe toutefois depuis les années 90**. L'intérêt d'une « *blockchain* privée » est simplement de permettre un horodatage, avec la preuve qu'une transaction est arrivée avant ou après une autre.

Algorithmes de consensus byzantin

Dans le modèle le plus simple, tout le monde est honnête, SI=on me dit 1 ALORS= je fais 1. Dans un modèle plus complexe, il existe des entités malignes qui veulent dévier le consensus de l'algorithme. Les modèles tolérants à ces entités malignes sont appelés algorithmes byzantins. Le modèle Bitcoin en est un, grâce à la preuve de travail.

Une des solutions classiques est appelé PBFT (Practical Byzantine Fault Tolerance) et permet de garantir le fonctionnement malgré un tiers de comportements malveillants.

2. M. Simon Polrot, avocat, fondateur d'Ethereum France et de VariabL

Simon Polrot a pour objectif de donner un panorama des différents projets *blockchain*, au-delà du bitcoin. Il commence par rappeler les objectifs de la *blockchain* et la définit comme **un registre d'identifiants et de transactions, distribué entre les participants et sécurisé par un protocole de consensus qui valide les nouvelles transactions**.

Distinctions publiques et privées

Selon lui, la distinction entre privées et publiques tient à l'ouverture, à l'identification des acteurs et à l'exercice ou non d'un contrôle, **mais aussi à l'utilisation ou non d'une cryptomonnaie comme méthode d'incitation**.

Minage

Le minage est un terme relativement impropre qui qualifie un processus par lequel les participants au réseau se mettent d'accord sur le dernier état de la *blockchain*.

La preuve de travail sur Ethereum permet de produire un bloc toutes les 15 secondes. **La preuve d'enjeu est une mise en gage d'une somme en cryptomonnaies**. Il existe des systèmes où l'on désigne des validateurs avec des votes et qui sont donc semi-centralisés.

Placer une limite haute pour la mise en gage permettrait certes d'éviter qu'un acteur s'accapare plus de 50 % du réseau, mais rendrait aussi plus facilement envisageable une attaque Sybil car on pourrait aisément en calculer le coût.

La blockchain privée est-elle une blockchain ?

La *blockchain* privée résout des problèmes d'infrastructure entre des parties prenantes qui ne font pas confiance à un organe centralisé. En termes sociétaux, la *blockchain* publique est plus intéressante à étudier car elle a beaucoup plus d'impact.

Nakamoto ne parlait même pas de *blockchain*, il n'utilise pas le terme dans son papier. Pour lui, l'innovation résidait dans un réseau qui échappe aux autorités.

Typologie de blockchains

Il existe différents usages et degrés d'utilisation de la *blockchain*, avec par ailleurs différents niveaux de sérieux.

1. *Blockchains* enregistrant des transactions simples en cryptomonnaies

Ex : Bitcoin, Bitcoin Cash, Litecoin ou deCRED.

Ce sont les plus éprouvées, les premières en termes de montant financier et les deuxièmes plus utilisées en termes de transactions, à ce jour.

2. *Blockchains* permettant d'émettre des actifs numériques (*tokens*) et de les échanger (plateforme *blockchain*)

Ex : Nem, NXT, Ardor.

Ces projets ont pour objectif de créer des nouveaux types d'actifs. Ils ont un usage marginal car ils sont d'une utilisation complexe.

3. *Blockchains* « nom de domaine »

Aujourd'hui le lien IP-nom de domaine est centralisé ; lorsque le serveur tombe en panne, le site tombe. Les registres de nom de domaine permettaient de sécuriser des URL mais ces projets ont quasiment disparu.

4. *Blockchains* « anonymes »

Ex : Monero, Zotero.

Ils permettent d'effectuer des transactions intraçables sur un registre distribué, avec des opérations cryptographiques très lourdes. Ils ne fonctionnent qu'à très petite échelle car les temps de calcul sont très importants.

5. Technologies décentralisées de stockage distribué

Ex : Storj.io, Sio, Filecoin…

Ce ne sont pas des *blockchains* à proprement parler et elles sont beaucoup moins efficaces qu'un hébergement centralisé.

6. *Blockchains* parodiques ou arnaques

Ex : Bitconnect, OneCoin, Dodgecoin…

Créées dans un but humoristique, ou pour mettre en place des arnaques à grande échelle.

7. *Blockchains* programmables

Ex : Ethereum, Tezos, Neo…

Au lieu d'avoir des instructions de script simples, comme le bitcoin, ces *blockchains* peuvent supporter des actions exécutables complexes. Ces programmes ont les caractéristiques des *blockchains* : publiques et vérifiables.

Smart contracts

Les *smart contracts* sont exécutés sur la *blockchain*, **ils permettent de prévoir l'exécution forcée d'un contrat dès lors que ses conditions sont remplies**. Pour cela il faut que toutes les composantes du contrat soient sur la *blockchain*. **L'oracle renseigne les informations nécessaires à déclencher le *smart contract***.

Les deux intérêts du *smart contract* sont **l'exécution forcée** d'un « contrat » et **l'auditabilité du code**. Exemples d'utilisations : contrats avec contrepartie financière, registre, *token*, ICO, OAD, dApps.

Les *smart contracts* peuvent effectivement permettre de déployer un registre sur la *blockchain*, ce registre peut s'administrer comme une base de données, donc avec une certaine rapidité.

dApps

Les dApps sont des applications d'Ethereum fonctionnant grâce à des programmes inscrits sur la *blockchain*, elles sont en réalité semi-décentralisées car elles nécessitent l'intervention d'un tiers.

Organisations autonomes décentralisées

Une DAO est une société dont toutes les règles de fonctionnement seraient inscrites sur la *blockchain*. Des *smart contracts* y administrent le dépôt de proposition, le vote, le paiement, les nominations…

Le projet le plus ambitieux à ce jour s'appelait TheDAO, il a échoué suite un piratage dû à une faille dans le code, qui a conduit à la perte de l'équivalent de 50 M$ en ethers. Cette perte représentait 5 % des ethers et a obligé à créer une *hard fork*, c'est-à-dire un retour de la chaîne Ethereum à un état antérieur.

Les DAO présentent-ils un risque de disparition de l'État ? Au moins du point de vue fiscal ?

Si toute la comptabilité d'une société est sur une *blockchain*, elle ne peut rien modifier après coup et ne peut rien cacher. C'est pourquoi, selon Simon Polrot, les DAO ne semblent être une menace ni pour les États, ni pour les institutions.

3. M. Pierre Porthaux, président de Blockchain Solution et d'EmergenceLab

Pierre Porthaux est ingénieur informaticien, titulaire d'un double diplôme de finance, il a travaillé plusieurs années dans le trading. Il dirige actuellement deux sociétés, Blockchain Solution, sa société de conseil et EmergenceLab, avec laquelle il a vendu une plateforme *blockchain* à un fond d'investissement.

Il concentre son intérêt sur le bitcoin car il est assez sceptique sur les potentialités des autres *blockchains*. Après un bref rappel historique sur le bitcoin et les motivations de Satoshi Nakamoto (circuit monétaire ouvert à tous, sans frontières et incensurable), il rappelle le fonctionnement élémentaire de la *blockchain*.

Selon Pierre Porthaux, dans le bitcoin **« *l'innovation c'est le consensus décentralisé, pas la blockchain* »**. L'idée de lier des blocs entre eux grâce à leur hash préexistait au bitcoin et est même très répandue (pour les dossiers de fichiers ou les git, par exemple).

Il vaut mieux utiliser le terme de **registre** plutôt que de base de données, car ce second terme a une acceptation précise et distincte en informatique.

Principes régissant le bitcoin

Bitcoin résulte de la combinaison de la théorie informatique (réseaux pair à pair et cryptographie) **et de la théorie des jeux** (incitations pour les mineurs à sécuriser le réseau).

Le bitcoin serait le seul jeu où l'on a intérêt à jouer dans les règles, celui qui ne joue pas dans les règles va non seulement ne pas gagner d'argent mais aussi en perdre (en dépensant de l'énergie en vain). Pour Pierre Porthaux, il ne peut y avoir de sécurité au système qu'en présence d'une cryptomonnaie pour récompenser les efforts des mineurs et créer de la compétition.

Changer un paramètre peut rendre le réseau extrêmement instable et il devient alors difficile de prédire comment il peut évoluer, car le système reste complexe. **Au fur et à mesure que le système croît il devient de plus en plus solide et les utilisateurs ont de moins en moins envie de prendre des risques en modifiant le code de base**.

Reproductibilité du modèle bitcoin

C'est pourquoi, dans le bitcoin le développement prend du temps, les développeurs les plus pressés proposent alors de créer leur propre *blockchain*… sur laquelle ils gardent la main. Or, une des raisons de la valeur des bitcoins c'est la confiance qui est accordée au réseau, et celle-ci résulte notamment de l'anonymat de Nakamoto et de l'autonomie du protocole. Les membres du réseau risqueraient d'avoir moins confiance si la *blockchain* était portée par un ou des développeurs identifiés.

Par ailleurs, les effets réseaux créés par le bitcoin sont extrêmement compliqués à recréer. C'est ce qui fait que les *tokens* et donc les ICO n'ont pas de valeur, car ils ne s'appuient pas sur une technologie prouvée dont on est sûr qu'elle fonctionnera. Les ICO dont on parle aujourd'hui ne sont pas nouvelles, elles existaient déjà dans les premières années du bitcoin.

Parce que la technologie n'est pas mature, beaucoup de ces ICO doivent être considérées comme des arnaques, avec des levées de fond énormes malgré peu d'informations et des systèmes trop complexes à mettre en œuvre. Il est très probable que les start-ups qui font des ICO auront du mal au final à être moins chères que d'autres utilisant d'autres technologies, et donc à dégager du profit.

En effet, le système *blockchain* n'est pas la panacée : *« **vendre une blockchain c'est bien, vendre une base de données la plus lente et la plus chère au monde, c'est autre chose** ».*

Sur les protocoles de preuve

La concentration et l'augmentation de la force de travail font partie des dérives qui n'ont pas été anticipées par Sakoshi Nakamoto (qui affirmait « un CPU, un vote »).

Cela dit, le protocole « *proof of work* » est objectif alors que tous les autres nécessiteront à un moment donné que quelqu'un arbitre les attributions de bloc. Plus fondamentalement, la *proof of work* est le lien entre le monde thermodynamique et le monde numérique. Ainsi, selon Pierre Porthaux : « ***On ne peut pas avoir et de la sécurité et des économies d'énergie*** ».

En résumé, tous les autres protocoles de consensus sont beaucoup plus complexes que celui de Nakamoto, et permettent souvent d'une manière ou d'une autre à une entité de contrôler le réseau. Il y aurait actuellement des investigations pour une *proof of work* moins énergivore.

Applications extra-monétaires

La *blockchain* est nécessairement lente car elle est décentralisée, l'information doit donc faire le tour du monde. D'un point de vue d'administrateur réseau, mécaniquement, un système décentralisé prend du temps. **Pour la même raison elle est limitée en capacité**. Ainsi, l'ajout de lignes de script, pour des *smart contracts* par exemple, est nécessairement complexe.

Le principal problème des *smart contracts* reste toutefois la dépendance à des facteurs exogènes, l'entrée de données dans le système. Il est donc nécessaire de réintroduire un tiers de confiance, il n'y a pas de *smart contract* automatique. Les *smart contracts* actuels sont donc des applications fonctionnant avec une base de données très lente, sans décentralisation.

« Je revis la même chose que lors de la bulle internet, certes il y a de très bonnes idées mais il faut rester réaliste ».

Blockchains privées

Pour les mêmes raisons de lenteur et de faible capacité, **l'intérêt des *blockchains* privées par rapport à d'autres solutions existantes est fortement discutable**. Beaucoup de projets de *blockchains* privées assez ambitieux se sont finalement rabattus vers les simples usages d'horodatage et d'ordonnancement.

Au-delà de l'aspect monétaire, l'intérêt principal de la *blockchain* est d'être une horloge universelle non centralisée. La production des blocs marque un rythme unique sur l'ensemble du globe, sans qu'une entité centralisée régisse ce mécanisme. **Cette horloge lente est le mécanisme le plus précieux qui soit dans le cadre d'un service décentralisé**.

La *blockchain* avec *proof of work* présente d'excellents cas d'usage en matière de preuve ou d'acte de notariat. On parlera ainsi de *prouvable computing* : en stockant dans la *blockchain* la preuve d'exécution d'une action, une entité est capable de prouver qu'elle a fait telle chose, à tel moment. C'est ce qui permet son utilisation par exemple dans des domaines qui nécessitent de la traçabilité. Valéria Faure-Muntian cite en illustration le cas de la *blockchain* alimentaire de Carrefour.

A la question de savoir s'il faudrait reconnaître l'opposabilité d'une preuve enregistrée dans la *blockchain*, Pierre Porthaux émet l'hypothèse que le régime actuel de reconnaissance légale de la signature électronique soit suffisant.

Dépasser les limites

Selon Pierre Porthaux, **il existe toutefois des solutions pour dépasser les limites des protocoles de *blockchain*, mais elles prendront plus de temps à émerger que ce qui est annoncé** par les promoteurs de la plupart des applications actuelles.

Internet repose sur des couches matérielles qui ne doivent surtout pas communiquer entre elles, c'est une erreur de placer la *blockchain* au niveau de la couche applicative alors qu'il s'agit en réalité d'une couche basse. **Cela amène à concevoir des applications trop sophistiquées répondant à des logiques directement commerciales, alors qu'il faudrait d'abord s'assurer de la fiabilité et de la solidité d'une *blockchain* simple**.

On peut établir un parallèle avec le rapport Théry qui comparait Arpanet et le protocole X25 (Minitel), en mettant en avant le second. Le protocole X25 était complexe, fermé, difficilement améliorable mais très axé business en proposant ce qu'il pensait être les applications du futur. D'autre part, on trouvait le protocole TCP/IP très « bête » et simple, sur lequel pourront finalement être construites toutes les applications actuelles d'internet.

Ethereum est en quelque sorte le minitel de 2017, il est trop intelligent, pas assez simple et ne permet pas à d'autres couches de se créer au-dessus du protocole existant. À titre d'exemple, concevoir un *Uber* décentralisé sur la *blockchain* aurait aussi peu de sens que d'évoquer un *Uber* décentralisé sur TCP/IP.

Développer des couches va prendre du temps, ainsi en 10 ans d'existence de Bitcoin, il a fallu attendre aujourd'hui pour que se développe la première application (litecoin). Pierre Porthaux n'est pas optimiste quant à l'avenir des solutions applicatives existantes, mais estime qu'à l'avenir d'autres pourront se développer sur une *blockchain* de base plus rudimentaire. **Il est tout à fait possible de construire des réseaux centralisés rapides sur des réseaux décentralisés plus lents, mais pas l'inverse.**

Selon Valéria Faure-Muntian, beaucoup des start-ups actuelles proposant des services *blockchain* sont des sociétés de conseil aux grandes entreprises historiques, qui viennent leur proposer des solutions que celles-ci ne pourront pas intégrer. D'ici quelques dizaines d'années, de nouvelles entreprises ayant intégré ces protocoles dès leur conception viendront détruire les anciennes.

Selon Pierre Porthaux, le secteur serait porté par une génération qui a « raté » le coche d'internet et qui ne veut pas prendre de risque pour cette innovation-là. Il reste que certains des domaines les plus cités sont aussi ceux où l'on se leurre le plus, en particulier dans le secteur bancaire. Ce secteur est en effet soumis à une forte réglementation et les banquiers ont besoin de connaître leurs clients.

La protection des données

La protection des données représente un vrai problème, sauf tant que l'on n'enregistre que les preuves et non les données en elles-mêmes. La *blockchain* publique du bitcoin n'est pas adaptée pour les problématiques de confidentialité.

Les autres technologies de registres distribués

Beaucoup d'autres modèles de registres distribués ont été des arnaques technologiques, ce fut le cas du projet IOTA. Cette initiative a échoué car la cryptographie n'était pas suffisamment solide, mais le code n'étant pas ouvert il est impossible d'en savoir plus. De manière générale, lorsque le code n'est pas public il faut se méfier. Cela dit, de

nouveaux projets vont forcément émerger car le code proposé par Satoshi Nakamoto n'était pas parfait.

Valéria Faure-Muntian conclut en soulignant l'enjeu pour la mission de baliser entre informations certaines et incertaines. Il s'agit en particulier d'éviter un nouvel « effet Minitel », en rejetant en bloc toute initiative, tout en évitant de rendre acceptable socialement des technologies qui pourraient être destructrices pour le consommateur final.

Selon Pierre Porthaux, la difficulté est d'autant plus grande que, comparativement à la création d'internet, les sommes mises en jeu sont bien plus importantes.

III. AUDITIONS DU 4 AVRIL 2018

1. M. Jean-Paul Delahaye, professeur d'informatique à l'Université de Lille I

Jean-Paul Delahaye tient à préciser qu'il n'est pas, à titre personnel, possesseur et spéculateur sur le bitcoin, ce qui a selon lui une certaine importance quant à l'objectivité de son expertise. Passionné en tant que mathématicien par les principes régissant le bitcoin et les protocoles de *blockchain*, il en a toutefois une vision critique, notamment du fait des enjeux énergétiques.

Définition de la blockchain

Pour définir la *blockchain*, Jean-Paul Delhaye cite Jean-Claude Trichet : « *La **blockchain** est une invention géniale, parce qu'elle repose sur une décentralisation complète de l'enregistrement des transactions. Au lieu d'avoir un système central qui enregistre et qui contrôle tout, on est en présence d'une technologie impressionnante testée sur beaucoup d'applications, qui n'ont rien à voir avec le Bitcoin*. » (2016, *Le Monde*).

Toutefois, la définition d'une *blockchain* reste complexe et sujette à discussion, ainsi les versions anglophones et francophones de Wikipedia à ce sujet divergent-elles nettement. Il n'en reste pas moins qu'il s'agit d'un **registre** (c'est-à-dire un fichier), **partagé** (c'est-à-dire que 5 000 nœuds détiennent ce registre) donc **infalsifiable** (protégé par des primitives cryptographiques) et **indestructible** (ou presque), et finalement composé de **blocs** (ou pages), successivement validés, datés et conservés par ordre chronologique.

Le critère de **l'ouverture**, c'est-à-dire de l'accessibilité et de la modification universelle, n'est pas systématique. Ainsi, par exemple, le *Ripple* (3^{e} crypto-actif en termes de capitalisation) est une *blockchain* fermée (*permissioned*) dont les nœuds sont des institutions financières identifiées, ce qui ne signifie pas pour autant qu'il y ait réapparition d'un tiers de confiance. Un des avantages de *Ripple* est qu'il ne nécessite pas de preuve de travail.

Au vu de la taille du réseau, dans le cadre de la preuve de travail et du minage, on sait que posséder 10 % de la puissance revient à obtenir au final 10 % des bitcoins produits.

Origine des blockchains

Le protocole Bitcoin a été défini en 2008 par un personnage qui se présente sous le nom de Satoshi Nakamoto**.** Nakamoto aurait travaillé deux ans à la conception du bitcoin. Même s'il garde l'anonymat, il s'agit probablement d'un groupe de plusieurs personnes qui possédaient des connaissances de très bon niveau en cryptographie.

Les spéculations sur son identité sont d'autant plus intéressantes que Nakamoto posséderait 5 % des bitcoins, c'est-à-dire environ 5 milliards de dollars aujourd'hui ! Les noms les plus cités sont les cryptographes et informaticiens Nick Szabo et Hal Finney.

Une technologie révolutionnaire ?

Avec internet, tout le monde peut être créateur et diffuseur de contenus, se débarrassant de la simple logique de « fournisseur vers client », il a rendu possible des modèles d'échanges entre pairs à grande échelle.

Tout ceci ne pouvait que s'appliquer un jour au modèle transactionnel : là où l'on croyait qu'il fallait obligatoirement un tiers de confiance**,** le modèle de la *blockchain* montre qu'il est possible de créer un pur modèle *pair* à *pair*. **En ce sens, la *blockchain* est la version transactionnelle des réseaux de pair à pair.**

Trois raisons expliquent que les *blockchains* soient apparues il y a une dizaine d'années et pas auparavant, il a fallu attendre :

- qu'une puissance de calcul et de mémorisation soit accessible largement grâce aux progrès des technologies de l'information (loi de Moore) ;

- la cryptographie mathématique moderne : même si de temps en temps une crypto est cassée, les méthodes actuelles de chiffrement ont potentiellement une durée de vie illimitée ;

- la technologie des réseaux pair à pair qui permettent de réaliser un partage d'informations collectivement validées et protégées. Cette construction collective d'une vérité commune, robuste et accessible à une large communauté, crée de la confiance et donc de l'efficacité.

Le bitcoin et les monnaies cryptographiques

Le bitcoin utilise quatre outils : les fonctions de hashage (SHA-256), les signatures à double clé (Elliptic Curve Digital Signature Algorithm, ECDSA), les incitations à surveiller la *blockchain* à travers le minage récompensé en unités monétaires et la preuve de travail pour attribuer les nouveaux bitcoins créés. **L'intuition révolutionnaire c'est l'ensemble du protocole dont les outils, pris indépendamment, étaient déjà connus.**

En septembre 2017, dans une conférence organisée par la Banque d'Angleterre, Christine Lagarde définit bien le bitcoin: « *Les monnaies virtuelles* [...] *produisent leur propre unité de compte et leur propre système de paiement. Ces systèmes permettent des transactions de pair à pair, sans chambre de compensation, sans banque centrale.* »

Elle explique aussi correctement, selon Jean-Paul Delahaye, pourquoi elles ne représentent pas pour l'instant de menace pour les monnaies classiques et les banques centrales : **«** *parce qu'elles sont trop volatiles, trop risquées, trop énergivores, parce que les technologies sous-jacentes ne sont pas suffisamment scalables, que beaucoup d'entre elles sont trop opaques pour les régulateurs et que certaines ont été piratées. Mais beaucoup de ces défauts ne sont que des défis technologiques qui pourraient être surmontés avec le temps*. »

Elle en tirait le 13 mars 2017 dans un article du FMI, les conclusions suivantes : *« Que la valeur de Bitcoin augmente ou qu'elle diminue, tout le monde se pose la même question : quel est exactement le potentiel des crypto-assets ? « La technologie derrière ces actifs, y compris blockchain, constitue une avancée passionnante qui pourrait aider à révolutionner*

d'autres domaines que la finance. [...] *Il ne serait pas judicieux de rejeter les crypto-assets* [...] *Nous pouvons exploiter le potentiel des crypto-actifs tout en veillant à ce qu'ils ne deviennent jamais un refuge pour les activités illégales ou une source de vulnérabilité financière. »*

À ce jour, la capitalisation des bitcoins (123 milliards de dollars) représentait un peu moins de la capitalisation totale des cryptomonnaies (271 milliards de dollars). **En sachant qu'il existe plus de 1 500 cryptomonnaies, les cinq de tête réunissent la plus grande part des actifs** (Bitcoin, Ripple, Ethereum, Bitcoin Cash et Litecoin).

Du 3 avril 2017 au 3 avril 2018, le cours du bitcoin est passé de 1 138 $ à 7 302 $, ce qui signifie que son cours a été multiplié par 6,2. En ce qui concerne l'ether, on observe même un facteur 8. Il est intéressant et surprenant de remarquer que toutes ces monnaies, y compris celles qui ont une structure très particulière (ex : Ripple), connaissent des cycles de variation parallèles.

Selon Jean-Paul Delahaye, certaines monnaies vont prendre de plus en plus d'importance, le bitcoin pour sa part va se tasser et laisser la place à d'autres, dont certaines ne sont pas aujourd'hui dans le top 10. Monero par exemple est une monnaie plus confidentielle que le bitcoin, qui ne permet pas de retracer les échanges.

Il reste important de comparer la masse du bitcoin avec d'autres véhicules financiers pour une juste mise en perspective : si le bitcoin vaut 141 Md$ et l'ensemble des cryptomonnaies 320 Md$, les dollars américains en circulation valent 1 500 $ et la capitalisation du marché de l'or, 8 200 $. Pour des activités frauduleuses, il reste bien plus pratique d'utiliser des dollars en liquide.

Événements récents

Il est important de suivre de près les événements qui animent le monde des *blockchains*. Pour cela il existe plusieurs sites anglophones et francophones (coindesk.com, cointelegraph.com, bitcoin.fr, journalducoin.com) qui produisent environ **5-6 articles par jour**.

Parmi les **événements notables**, on **retiendra en particulier** :

- Le 24 août 2017 : un ajustement technique du bitcoin avec l'adoption de ***Segregated Witness*** (BIP141), qui permet d'accueillir plus de transactions en un bloc.

- Le 1er août 2017, est proposée la hard fork **Bitcoin Cash**, qui ne sera pas suivie par la majeure partie des nœuds. Apparaît alors une seconde chaîne, où la taille des blocs passe de 1 méga-octet à 8 méga-octets (la taille des blocs ne ralentit pas les fonctions de hashage car seule la tête des blocs est hachée).

Étonnamment, les prévisions catastrophistes des opposants aux *hard forks* ne se sont pas réalisées. En effet, on aurait pu imaginer qu'en divisant le réseau, chacun des réseaux créés le serait avec une force moindre, donc avec un niveau de confiance moindre et finalement un cours à la baisse. En réalité, l'intense volatilité des cours a largement compensé cet effet et Bitcoin Cash vaut aujourd'hui 951 dollars, **l'addition des valeurs des deux chaînes est donc finalement plus importante que la valeur de la chaîne originelle**.

Autre fait étonnant, si le réseau s'est fissionné, les transactions originelles communes sont toujours inscrites dans la *blockchain*. Des possesseurs de bitcoin avant la fission se sont donc retrouvés propriétaires de bitcoin et de bitcoin cash car toutes ces transactions ont été dupliquées. En théorie, ce n'est pas un enrichissement puisque la valeur de chacune de ces transactions aurait dû diminuer.

- Le 24 octobre 2017, apparaît la fork **Bitcoin Gold** qui veut établir une nouvelle preuve de travail, Equihash, elle est nettement moins suivie. Le Bitcoin Gold vaut ainsi aujourd'hui 65 dollars (21e).

- Courant 2017, **le gouvernement chinois interdit les plateformes d'échange et le minage**, ce qui ne semble pas encore particulièrement faire effet.

- Le 10 décembre 2017, **la Bourse de Chicago reconnaît des contrats à terme sur le bitcoin**, ce qui apparaît pour certains comme une « officialisation » de la cryptomonnaie.

- Courant 2017, apparaît aussi la **prise de conscience mondiale du coût électrique** du fonctionnement du Bitcoin.

- En mars 2018, Facebook, Google, Twitter refusent les publicités pour les monnaies cryptographiques et les ICO.

- Le 10 mars 2018, Wall Street Analyst publie le « Bitcoin Misery Index » for Traders.

- Le 15 mars 2018, l'AMF publie une liste noire de sites d'investissement en crypto-actifs.

Huit problèmes pour les monnaies cryptographiques

Malgré sa solidité apparente, le bitcoin présente plusieurs problèmes d'importance variable.

Problème 1 : Une volatilité déraisonnable

Le cours du bitcoin a pu être multiplié par 14 en 2017, ce qui est bien plus que l'ether. Du 17 décembre 2017 au 2 avril 2018, la valeur du bitcoin a baissé des deux tiers, il est arrivé que le cours gagne ou perdre 20 % en une journée.

Pour certains (dont Jean-Claude Trichet), cette volatilité signifie que le bitcoin n'est pas une monnaie, toutefois elle a tendance à s'atténuer. Deux points de vue s'opposent ici : pour certains la non régulation des cryptomonnaies a pour conséquence inévitable leur volatilité ; pour d'autres, dont Jean-Paul Delahaye fait partie, une fois une masse monétaire assez importante atteinte, la volatilité se calmera. Ainsi, à titre de comparaison, l'or n'est pas régulé mais sa volatilité est assez raisonnable.

Problème 2 : Un faible nombre de transactions possibles

La scalabilité est probablement le plus gros problème du bitcoin et des *blockchains*. Le bitcoin ne permet ainsi que de cinq à dix transactions par seconde (quatre en moyenne, 350 000 par jour). Comparé à beaucoup d'autres moyens de paiement, c'est infiniment peu. Par ailleurs, il arrive que le réseau bitcoin soit gravement saturé durant certaines périodes.

Cela a eu pour conséquence des transactions bloquées : jusqu'à 100 méga-octets de transactions en attente (12-2017) et une attente de plusieurs jours en l'absence de commission suffisante, et des commissions importantes : jusqu'à neuf bitcoins par page et jusqu'à 50 dollars par transaction.

Cela rend impossible pour l'instant les applications fondées sur des micro-transactions comme le petit commerce, l'horodatage, les ancrages ou les preuves d'existence.

Plusieurs solutions ont pu être envisagées :

- les ***blockchains* alternatives** comme Bitcoin Cash permettent une augmentation de la taille des pages mais l'effet est limité et ne permet pas une multiplication par 100 ou 1 000 comme cela serait nécessaire pour égaler la puissance d'un réseau de cartes bancaires ;

- les **sidechains** lient plusieurs *blockchains* ayant des fonctions différentes les unes aux autres. Étonnamment, elles ne semblent pas se mettre en place, cela peut être dû à des difficultés techniques ou au refus (implicite) du réseau bitcoin de faire les modifications nécessaires ;

- le **lightning network** consiste à créer une nouvelle couche sur le protocole bitcoin mais il n'est pas certain que cela marche vraiment et certains avantages des *blockchains* sont perdus au change, en particulier en termes de sécurité ;

- les **modèles non-*blockchain*** (hgraph, Cardano, etc.) doivent faire leurs preuves mais sont porteurs d'espoir ;

- les ***blockchains* fermées** (« permissioned », Ripple) semblent marcher mais ne sont pas utiles pour tous les cas d'usage.

Problème 3 : Un bug possible dans le code

On dit souvent de manière erronée que le protocole Bitcoin tient depuis 2009 ; en effet, il a été attaqué avec succès le 15 août 2010 lors de l'accident appelé « *value overflow* ».

En résumé, le 15 août 2010, a été découvert un bloc contenant une transaction créant 184 milliards de bitcoins. L'erreur provient de ce que le code utilisé pour vérifier les transactions avant de les inclure dans un bloc ne prenait pas en compte des valeurs aussi grandes.

Une nouvelle version du client pour corriger ce bug de dépassement de capacité est publiée dans les cinq heures suivant la découverte du bug, rejetant toute transaction de plus de 21 millions de bitcoins. De nombreux nœuds non corrigés continuent à construire la « mauvaise » *blockchain* pendant de nombreuses heures. Finalement, la « bonne » *blockchain* finit par s'imposer, ce qui provoque l'annulation des transactions frauduleuses, mais aussi d'autres transactions.

Problème 4 : Des attaques possibles des primitives cryptographiques

Les courbes ECDSA (Elliptic Curve Digital Signature Algorithm) sont en danger à plus ou moins long terme. Adi Shami, cryptographe reconnu à l'origine du fameux algorithme RSA, a fait des prédictions concernant le futur de la sécurité informatique, parmi lesquelles celles-ci :

6. *Elliptic curves will fall out of favour.* NSA *moving away from it with no explanation*.

13. *Bitcoin will fade away but leave a legacy*

Par ailleurs, le SHA-256 pourrait être attaqué, des algorithmes de hachage l'ont déjà été et ont été cassés (partiellement ou totalement). Cela pourrait très bien arriver à SHA-256, ce qui aurait de très graves conséquences. Le SHA1 a ainsi été attaqué par Google, une collision a été trouvée en 2017.

Problème 5 : les attaques 51 %

Les nœuds principaux du réseau (les mineurs) qui le surveillent et le font fonctionner sont rémunérés. Toutes les 10 minutes, l'un d'eux gagne 12,5 bitcoins. Il est tiré au sort selon une méthode telle que plus le mineur est capable de calculer SHA-256, plus il a de chances de gagner.

Ainsi, un acteur détenant plus de 50 % de la puissance du réseau peut secrètement créer une « fausse *blockchain* » (par exemple pendant 10 heures) puis la rendre visible, ce qui a pour effet de la rendre dominante car elle possède un contenu en calcul supérieur à la « bonne *blockchain* ». Les pages des 10 dernières heures de la « bonne *blockchain* » sont alors annulées.

On parle ici d'attaque « Goldfinger », le but n'est pas tant de gagner de l'argent en faisant des double dépenses (car de toute façon l'opération serait difficilement rentable), mais plutôt de porter atteinte à la confiance que les usagers placent dans le réseau.

Elle aurait effectivement un coût très élevé (quelques milliards) mais est à la portée d'un État ou des grosses firmes. Par ailleurs, étant donné qu'encore à ce jour 60 % à 70 % du minage se fait en Chine, le gouvernement chinois, en exerçant son autorité sur les mineurs chinois, peut donc faire tomber le bitcoin quand il le souhaite.

Problème 6 : La dépense électrique

L'énergie dépensée par le minage rend impossible d'envisager que Bitcoin rivalise un jour avec le dollar, l'euro ou l'or. Aujourd'hui les réseaux Bitcoin dépensent au strict minimum l'équivalent de la production de trois centrales nucléaires de 8 TWh (mais plus probablement six ou sept centrales, soit plus de 10 % de la production électrique française).

Les méthodes d'estimation sont source de nombreuses discussions, mais le calcul minorant est simple et incontestable. Il est réalisé à partir des caractéristiques de l'outil de minage énergétiquement le plus efficace du marché, *Antminer S9*, qui produit $13{,}5*10^{12}$ hash par seconde pour une dépense électrique de 1,323 W.

La puissance du réseau bitcoin au 2 avril 2018 est de $28*10^{18}$ hash par seconde. Si tout le minage était fait *Antminer S9*, il faudrait 2 074 000 appareils. La consommation totale de ces appareils serait de 2,743,000,000 W. Ce que l'on ramène annuellement à 24 TWh, soit environ trois centrales nucléaires.

D'autres méthodes de calcul existent, on peut notamment estimer que les mineurs investissent pour leurs opérations une somme proche des récompenses qu'ils touchent. C'est l'hypothèse du *digiconomist* qui propose une valeur de 58 TWh (soit sept centrales) à la même date. À titre de comparaison, l'ensemble des data center de Google représentent 6 TWh, toutes les télévisions de France, 3 TWh.

Pour égaliser la masse monétaire de l'or il faudrait entre 1 000 et 2 000 TWh (par la méthode du calcul gain=dépense), ce qui représente une multiplication par 60 de la puissance de calcul nécessaire, c'est-à-dire 180 centrales nucléaires.

Pour justifier le coût électrique du minage, plusieurs faux arguments sont parfois présentés :

- les processeurs de SHA-256 progresseraient, ce qui diminuerait ce coût. Cet argument est faux car tout le monde progresse en même temps, que ce soit les mineurs ou les attaquants 51 % ;

- l'électricité utilisée ne vaudrait presque rien, car produite en surplus, proche des fermes de minage, ou encore il pourrait s'agir d'énergie verte et l'on pourrait aussi réutiliser la chaleur produite pour la revendre. Dans toutes ces options, tout attaquant 51 % peut faire de même : utiliser de l'électricité verte ou à bas coût, ou revendre de la chaleur.

En effet, le minage ne protège des attaques 51 % que s'il coûte de l'argent, suffisamment pour dissuader les attaquants 51 % d'en mettre autant sur la table. La dépense électrique est liée à la compétition.

Cette dépense électrique aura des conséquences politiques à moyen terme car si le cours des monnaies cryptographiques basées sur des preuves de travail devait augmenter, la dépense électrique qui lui est liée aussi, et cela aura un impact sur le prix de l'électricité.

Déjà en février 2018, la ville de Plattsburg dans l'État de New-York a interdit pendant 18 mois l'installation de nouvelles usines de minage, car leur présence avait fait augmenter le prix de l'électricité pour les usagers. De même, en avril 2018, la police sud-coréenne a arrêté une quarantaine de mines illégales.

Problème 7 : Le modèle de gouvernance est mal pensé

Aujourd'hui, ce sont les mineurs qui détiennent l'essentiel du pouvoir d'évolution du protocole, et ils ne veulent pas le changer. **Ils ne voudront en particulier surtout pas abandonner les systèmes de preuves de travail avec du SHA-256 car ils ont investi des milliards de dollars en matériel spécialisé**.

Problème 8 : Les usages frauduleux du bitcoin

Le bitcoin est de l'argent liquide numérique, en cela il est plus commode que les billets. Cela rend plus facile des usages frauduleux de toutes sortes. Pire encore, cela rend possible de nouveaux usages frauduleux comme la demande de rançon (« *ransomware* »), pour les trafics divers ou le blanchiment.

2. M. Manuel Valente, directeur de La Maison du Bitcoin

Manuel Valente annonce faire une présentation sur l'infrastructure des projets *blockchains* et sur sa gouvernance. Il est directeur de La Maison du Bitcoin, lieu physique consacré aux crypto-actifs à Paris, premier du genre en Europe.

Les programmeurs du bitcoin

Manuel Valente propose une définition de la *blockchain* comme un réseau sans contrôle de quiconque ni entité centralisée, dont le système évolue par consensus, c'est-à-dire lorsqu'une très large majorité des membres se mettent d'accord.

Par analogie avec le système législatif, les programmeurs seraient ceux qui suggèrent une nouvelle loi, les nœuds ceux qui votent pour ou contre celle-ci, et les mineurs ceux qui l'appliquent.

Les programmeurs du bitcoin correspondent à un noyau dur d'une quarantaine de développeurs, dont les membres sont repérés pour leurs propositions pertinentes de

modification. Ils sont donc cooptés et sélectionnés pour leur valeur technique. Ce modèle se retrouve classiquement dans le développement des programmes libres comme le système d'exploitation *Linux*, entre autres.

Certain travaillent bénévolement pour la mise en valeur personnelle que permet une participation au code du bitcoin, toutes leurs modifications étant visibles sur la page Bitcoin du site de développement participatif github.com. D'autres sont financés par des entreprises qui ont un intérêt dans le développement de Bitcoin, dont la plus importante est Blockstream.

L'évolution du code fonctionne à partir des propositions d'évolution avancées par les développeurs principaux ou par des développeurs occasionnels, c'est le Bitcoin Improvement Proposal. Ces propositions, implémentées en code informatique, sont discutées publiquement. Depuis le début du bitcoin, sur 174 propositions créées, seules 13 ont été acceptées, ce qui témoigne de la dimension assez conservatrice de l'écosystème du bitcoin.

Le choix des modifications

Malgré tout, les programmeurs n'ont qu'une force de proposition, et **c'est aux 10 à 15 000 nœuds de choisir si une modification sera adoptée ou non.** Est un nœud tout ordinateur connecté à internet qui contient le protocole à jour et une copie intégrale de la *blockchain*, chacun est connecté à une dizaine d'autres nœuds. Les clients qui font des transactions et possèdent des portefeuilles de crypto-actifs sont connectés à ces nœuds qui servent de point d'accès à la *blockchain*.

Ces nœuds sont les référents du protocole et de l'historique, la version la plus valide du protocole est celle qui est partagée par tous les nœuds. Cela signifie que **chaque nœud, en décidant individuellement d'accepter ou non une modification (qui prend la forme d'une simple mise à jour), vote pour ou contre l'application de celle-ci à l'ensemble du réseau**. Lorsqu'une large majorité de nœud a adopté une modification, le réseau fonctionne alors sous le régime des nouvelles règles qu'elle instaure.

Certaines modifications sont conçues de telle sorte que **les blocs fabriqués sous une nouvelle version peuvent être validés par les nœuds qui restent sur l'ancienne version**, **on parle alors de *soft fork***. D'autres rendent les blocs minés sous les nouvelles règles impossible à valider par les nœuds n'ayant pas installé la mise à jour, on dit qu'**il n'y a pas de rétrocompatibilité et se crée alors une *hard fork***.

Lorsque le consensus n'est pas massif en faveur ou en défaveur d'une modification, et qu'une grande proportion des nœuds a accepté la mise à jour tandis qu'un grand nombre d'autres l'a refusée, **il peut apparaître une nouvelle *blockchain* fonctionnant indépendamment**. Cela est arrivé à plusieurs reprises car la *blockchain* du bitcoin présente des limites, notamment en matière de taille de blocs, qui est limitée à 1 Mo, ce qui engendre des **problèmes de scalabilité**. Ainsi plusieurs développeurs du bitcoin ont proposé des améliorations qui ont été refusées par une majorité plus conservatrice.

Le minage : intérêt et répartition

Les mineurs de la *blockchain* ont un rôle proche d'une chambre de compensation, ils vérifient la validité et la solvabilité des transactions avant de les ajouter dans des blocs qu'ils créent. Ils fournissent ensuite aux nœuds les transactions validées. Ils ont deux sources de rémunération : les commissions de transaction et la création monétaire par le protocole lui-même. L'analogie avec les métaux précieux vient de ce qu'ils « travaillent » pour obtenir quelques rares blocs très valorisés.

Le minage joue un rôle fondamental pour l'immuabilité de la *blockchain*, il ne peut fonctionner sans récompense (création monétaire et commissions) car la preuve de calcul est onéreuse, ils ont un impact fort sur l'évolution du protocole car ils peuvent choisir ou non de valider des blocs sous un nouveau format de règles. Dans les *blockchains* privées il n'y a pas de minage, l'immuabilité n'est donc pas forcément garantie.

Aujourd'hui, les principales fermes de minage se trouvent en Chine, en Géorgie, aux États-Unis, au Canada et en Suède. Le Kazakhstan révèle être de plus en plus ciblé par les investisseurs en raison du coût très faible de son électricité. À l'inverse, la France ne présente pas des conditions optimales pour le minage. Néanmoins **il existe trois *pools* de minage français : Big Block Data, Wizard Mining et Just Mining**.

Le minage: consommation énergétique

La consommation électrique de la *blockchain* du bitcoin ne dépend pas du nombre de transactions mais de la preuve de travail. Plus il y a de mineurs dans le système, plus sa difficulté va augmenter. Il se produit un équilibre entre les dépenses des mineurs pour obtenir de la puissance de calcul, et le revenu qu'ils peuvent espérer en récompense de leur production de blocs.

Il est à noter que l'incitation monétaire est divisée par deux tous les 210 000 blocs, c'est-à-dire tous les quatre ans. On peut s'interroger sur le fait que les mineurs pourraient en compensation augmenter les frais de transaction.

Le 4 avril 2018, le minage du bitcoin exigeait 28 milliards de milliards de calculs par seconde, sa traduction en termes de consommation énergétique varie sensiblement selon les modes de calculs : de 20 TWh/an (Bloomberg) à 140 TWh/an (Morgan Stanley), en passant par 60 TWh/an (Digiconomist).

Le minage est certes très énergivore mais on observe plusieurs facteurs de réduction de cet impact, comme l'utilisation d'énergie verte, la récupération de chaleur ou l'optimisation de la production électrique en surplus (appel d'offre d'Hydro-Québec pour ses barrages). Ainsi, en mars 2018, a été inauguré en Norvège un centre de minage par le ministre du commerce et de l'industrie, utilisant de l'énergie verte et créant 30 emplois.

Le minage : développement et équilibre financier

Pour calculer la rentabilité du minage, on peut utiliser comme référence la machine la plus performante (*Antminer S9*), pour estimer le coût total minimal du minage avec un coût de l'électricité donné : (25 000 000 TH/s/14 TH/s) * 1,4 kW * 0,10€/kWh = 250 000 €/h. À comparer avec le revenu minimal global par heure, qui se calcule à partir de la récompense (12,5 BTC) et une valeur basse du cours du bitcoin : 12,5 btc/block * 6 block/h * 6000 €/btc = 450 000 €/h.

Ainsi la rentabilité dépend de multiples facteurs : le cours du bitcoin, le prix de l'électricité, l'efficacité des machines, les coûts additionnels : refroidissement, locaux, salaires, achat du matériel...

La puissance de calcul augmentera tant que l'équilibre de rentabilité penchera en faveur du minage, mais cessera lorsque les coûts et revenus s'équilibreront. La puissance de minage actuelle semble rejoindre cet équilibre et ne devrait pas augmenter beaucoup plus à l'avenir, d'autant plus que les revenus sont divisés par deux tous les quatre ans.

En toute hypothèse, **les coûts de fonctionnement sont importants car ils constituent le sous-jacent physique du crypto-actif généré**.

Alternatives à la preuve de travail

Des alternatives à la preuve de travail sont toutefois envisagées :

- la **preuve d'enjeu**, qui consiste à ce que des nœuds gardent en séquestre un montant de crypto-actifs et que parmi eux soit choisi un mineur. Cette solution n'est toutefois pas encore tout à fait prouvée et des risques d'exploitation malveillante existent ;

- la **preuve de capacité**, qui consiste à mettre en gage de l'espace disque disponible ;

- la **preuve de destruction**, qui revient à détruire des crypto-actifs pour obtenir la confiance du réseau.

Tous ces systèmes supposent toutefois la confiance en un acteur.

Conclusion

La collaboration de trois types d'acteurs (programmeurs, nœuds et mineurs) garantit le fonctionnement des *blockchains* publiques, leur interdépendance est garante du principe de décentralisation.

3. M. Gérard Memmi, responsable du département informatique de Telecom ParisTech

Gérard Memmi débute son intervention par un rappel des principes régissant la *blockchain* qu'il décrit **un livre de compte où l'on ne peut ni modifier, ni supprimer l'information.**

Selon lui, les critères qui sont requis pour une *blockchain* fonctionnelle sont les suivant :

- un registre répliqué qui n'autorise que l'ajout irréversible de données ;

- une cohérence des données, en particulier les *smart contracts* qui doivent être valides ;

- une protection des données.

Dans une base de données classique, il est possible de garantir ces propriétés en contrôlant l'accès du registre, ce qui suppose d'avoir confiance en l'entité qui le maintient.

La solution des *blockchains* revient à décentraliser et répliquer le maintien du registre entre plusieurs lieux. Ainsi les entités participantes n'ont pas besoin d'avoir confiance entre elles, cela fonctionne tant que suffisamment d'entités sont effectivement susceptibles de confiance et ne forment pas de coalitions (de plus de 51 %). Cette honnêteté est motivée par une récompense pour la production de blocs qui sont protégés par des moyens cryptographiques. L'ensemble de ces blocs est répliqué dans un réseau P2P (sans nœud central), évitant un point unique de défaillance.

La ***blockchain* initiale de Satoshi Nakamoto était *permissionless***, c'est-à-dire que n'importe qui pouvait participer au maintien du registre, sans besoin de s'enregistrer au

préalable. Cela impliquait un fonctionnement efficace quel que soit le nombre d'entités participantes.

Par la suite, une variation plus adaptée à certaines applications a vu le jour : les ***blockchains* de consortium**, où les entités participantes sont enregistrées au préalable. Le registre peut être plus rapide et plus fiable, en étant toujours contrôlé par la majorité des participants.

Applications

De manière générale, la *blockchain* est une solution adaptée dans les cas où :

- **plusieurs acteurs veulent consigner des événements** ;

- ces événements ont un caractère **irréversible** (traçable ou auditable) ;

- ces acteurs ont **des intérêts potentiellement conflictuels** ;

- ceux-ci peuvent être très nombreux et ne pas être connus à l'avance ;

- ils ne veulent pas compter sur un arbitre toujours actif, c'est-à-dire **un tiers de confiance**.

Ainsi, à titre d'exemple, le laboratoire CEIDO (commun à Telecom ParisTech et EDF) développe une place de trading d'énergie, basée sur des *smart contracts* et la *blockchain* Ethereum. Ce projet a vocation à s'étoffer avec le support de Mines ParisTech qui va introduire de nouveaux algorithmes en théorie des jeux (référent : Georges Kariniotakis).

Dans une application de cryptomonnaies, le registre stocke des ordres de transactions, il est validé par les mineurs si son émetteur dispose de suffisamment de fonds non déjà dépensés.

Il est à noter que de nombreuses organisations soutiennent le développement de *blockchains* : EEA, Hyperledger, R3, Axoni, Chain, ou encore Digital Asset sont financées par JP Morgan, BoA, WF, CitiGroup et GolmanSachs. De leur côté, Cisco, IBM, Intel et Microsoft développent un consortium.

Smart contracts

Grand domaine d'application des *blockchains*, les *smart contracts* sont de simples programmes implémentés sur une *blockchain*, historiquement sur Ethereum mais maintenant développés sur des *blockchains* dédiées partout dans le monde.

Il est possible de faire cohabiter plusieurs *smart contracts* sur une même *blockchain*. Du point de vue de celle-ci, chaque application ne diffère que par son prédicat de validation. Toutefois, maintenir une *blockchain* par application est coûteux.

Les *smart contracts* sont porteurs de beaucoup d'espoirs mais présentent tout de même d'importantes problématiques liées à ce que par définition, le code inscrit sur une *blockchain* ne peut pas être modifié. Cela rend les erreurs de programmation ou d'interprétation (bugs), communes à tout développement informatique, bien plus pénalisantes. Cela implique aussi que les utilisateurs puissent avoir des résultats inattendus.

Les premiers langages permettant de développer des *smart contracts*, *Solidity* pour Ethereum et *Fabric* pour Hyperledger ont été créés en quelques mois, bien plus rapidement que ce qui est habituel en matière de création de langage. Ils se sont exonérés de la définition

d'une sémantique formelle, ce qui est à l'origine de nombreuses erreurs de compilation. **De fait, on ne peut pas dire aujourd'hui que les *smart contracts* soient au point techniquement.**

Les chercheurs sont en train de remédier à ces problèmes qui demandent des connaissances très poussées en informatique théorique, pour prouver les *smart contracts* qui sont écrits afin qu'ils fassent bien ce pour quoi ils sont prévus. Il s'agit d'écrire une sémantique formelle et par la suite de développer des compilateurs correspondants.

Les principaux pôles de recherche dans ce domaine sont aux États-Unis (MIT, Cornell…), en France (INRIA principalement) et en Israël, mais aussi au Royaume-Uni.

Preuve de travail et consommation d'énergie

Dans les *blockchains proof of work*, les entités participant au maintien du registre sont les mineurs, chaque entité est représentée par sa puissance de calcul et le contrôle d'accès au registre est distribué au prorata de la puissance de calcul disponible.

De par leur design, les *blockchains proof of work* requièrent une grande consommation d'énergie, celle-ci est directement liée au coût d'une prise de contrôle unilatérale du registre. En effet, la seule contrainte sur ce coût est qu'il doit être suffisamment élevé pour dissuader n'importe quel attaquant.

Cela dit, il est difficile, voire impossible, d'estimer un coût minimum, de fait celui-ci est rendu aussi grand que possible et les mineurs se livrent une compétition féroce. Il est possible de consulter la répartition des *pools* de minage sur *https://blockchain.info/fr/pools*. Les plus importants se trouvent en Chine car c'est là que sont fabriquées les machines permettant le hashage à très grande vitesse, et l'électricité y est peu chère.

Aujourd'hui, la consommation du minage de bitcoin est comparable à la consommation électrique de la Colombie ou de la République tchèque. Le bitcoin consommerait à lui seul 0,13 % de l'électricité produite dans le monde, à comparer avec les 2 % que représente la totalité des systèmes informatiques mondiaux. Il est difficile de faire des projections d'évolution, mais on peut noter qu'au cours du dernier mois (mars 2018), la consommation d'énergie du bitcoin a augmenté de 30 %.

Pour calculer la consommation énergétique mondiale minimum, on peut faire un calcul simple en se référant à la consommation d'*Antminer S9*, la machine à hasher la plus efficace du marché. On note une évolution très rapide de ces machines, ainsi *Antminer S1* en 2014 avait une puissance de 180 GHashs/s, là où le *S9* déploie une puissance de 14TH/s. Cette évolution devrait se poursuivre car si le *S1* utilisait un processeur à échelle 55nm, le S9 est à 16nm et la prochaine génération qui devrait sortir cette année sera à 7nm, donc encore plus rapide.

Ces machines coûtent autour de 2 000 € et sont consacrées uniquement au calcul de hashs, avec une vitesse sans comparaison possible avec un CPU classique ou à une carte graphique. Sony, TSSC, Intel ou GMO en sont les principaux constructeurs.

D'autres limites hors consommation d'énergie

La plupart des limites actuelles sont liées à un manque de maturité technologique, mais des améliorations importantes sont faites dans plusieurs propositions récentes. Une des caractéristiques qui peut être évitée est la lisibilité totale des données du registre par tous les participants, mais au prix de nombreuses contreparties.

Enfin, le stockage toujours croissant (sans suppression ni archivage des premiers blocs) de l'ensemble du registre peut devenir prohibitif pour les nœuds.

Le projet BART

Lancé le 6 mars 2018 avec Inria, Télécom ParisSud, Télécom ParisTech et SystemX, le projet BART (*Blockchain Advanced Research & Technologies*) vise à regrouper toute la recherche sur les *blockchains* en un lieu sur le plateau de Saclay. Aujourd'hui, les premières initiatives sont de l'ordre de l'organisation d'un workshop annuel (co-sponsorisé par SEIDO/EDF), de séminaires scientifiques (INRIA et X), de cercles de lecture et le recrutement de premiers doctorants.

Ce projet a établi une feuille de route qui vise à répondre aux principaux défis technologiques des chaînes de blocs, concernant :

1. les **modèles théoriques**, en particulier l'écriture et la preuve de nouveaux langages de programmation des *smart contracts* ;

2. le **passage à l'échelle** (scalabilité) grâce à l'hybridation, c'est-à-dire des *blockchains* qui communiquent entre elles et la hiérarchisation (en coopération avec l'Université Technique de Munich, *Technische Universität München* ou TUM) ;

3. la sécurité de bout en bout, c'est-à-dire portant autant sur les clients logiciels que sur le matériel sur lequel repose la *blockchain* (*hardware*) ;

4. les **architectures, qui concernent l'interopérabilité de la *blockchain* avec le monde extérieur**. Cela suppose qu'elle s'inscrive dans une vision globale avec l'internet des objets, le BigData, l'intelligence artificielle… En France, l'INRIA et le CEA sont en pointe sur ces questions ;

5. la **confidentialité des données**, avec la fragmentation et le chiffrement ;

6. les **modèles économiques et la régulation**, en travaillant sur de nouveaux modèles d'affaire et sur l'impact social.

Quelques exemples de sujet traités par le projet BART :

- **Renforcer la sécurité et la traçabilité des transactions**. Dans la *blockchain* actuelle les wallets sont constitués d'adresses munies de clés cryptographiques symétriques et qui posent un double problème : l'attribution anonyme d'adresses et la sécurité des clés généralement hébergées sur des serveurs et protégées par un couple login/mot de passe ; lorsque ces clés sont perdues, on perd toute possibilité d'accès à la *blockchain*. Il s'agit de définir des systèmes ayant une sécurité similaire par exemple au réseau bancaire actuel pour les paiements.

Deux solutions sont possibles et étudiées : le chiffrement homomorphique et le *multiparty computing*, où l'on fragmente la donnée avant de la chiffrer, afin de se prémunir d'une attaque durant la phase de chiffrement.

- **Valider la *blockchain* en consommant moins d'énergie**, en étudiant différentes solutions possibles :

- le passage de la POW à la POS ou à un autre type de preuve de validation (volet conduit avec la *Technische Universität München* ou TUM) ;

• une compilation basée sur du profilage énergétique (volet conduit avec MinesParisTech).

- **Permettre la montée en charge**, en étudiant de nouvelles architectures (volet conduit avec TUM et SystemX) :

• la hiérarchie (conservation et archivage), permettrait de se débarrasser de certains blocs plus anciens ;

• l'hybridation en superposant et intégrant à la *blockchain* un logiciel complémentaire (lightening, sidechain…).

IV. AUDITIONS DU 24 MAI 2018

1. M. Jean Zundel, spécialiste d'Ethereum

Pour Jean Zundel, une *blockchain* est un **réseau** de **consensus crypto-économique**. Réseau, car il s'agit d'échanges entre nœuds en *peer to peer*, fonctionnant par consensus, car il n'y a pas de divergence, qui utilise la cryptographie, ce qui garantit l'historique et une incitation économique qui garantit la pérennité.

Pour lui, les crypto-actifs sont des monnaies au sens d'Aristote, c'est-à-dire des unités de compte, des réserves de valeur et des moyens d'échange. Selon les monnaies, il y a un compromis à établir entre réserve de valeur et moyen d'échange.

Émission et usage de la monnaie

La monnaie d'Ethereum, l'ether, a la particularité d'avoir une émission continuelle et non régressive, contrairement à d'autres cryptomonnaies qui ont une limite de volume prédéfinie.

La rareté donne de la valeur, il y a un lien entre tendance déflationniste ou inflationniste d'une monnaie et le fait qu'elle va servir plutôt comme un moyen d'échange ou comme une réserve de valeur. Le bitcoin ayant une émission limitée va devenir de plus en plus rare. On peut le considérer comme une forme d'« or 2.0 », une réserve de valeur que l'on va avoir tendance à conserver et à ne pas utiliser au jour le jour.

L'ether devrait lui aussi rester une réserve de valeur parce que l'émission continuelle est censée compenser les ethers perdus ou brûlés, mais c'est avant tout un **moyen d'échange**.

UTXO

Ethereum n'utilise pas d'*Unspend Transaction Output (UTXO)* pour gérer les soldes et balances, contrairement au bitcoin.

Dans le système Bitcoin, chaque transaction se fait à partir d'un compte (*output*) déjà présent dans les portefeuilles des utilisateurs. Si un utilisateur qui possède un compte de 0,1 BTC veut donner 0,4 BTC à un autre, la transaction consistera en la création de deux nouveaux comptes. D'une part, un compte de 0,4 BTC qui sera encrypté au bénéfice du destinataire de la transaction, d'autre part un compte « non-dépensé », un UTXO, qui sera encrypté au bénéfice de l'émetteur.

L'avantage des UTXO c'est qu'ils permettent facilement d'éviter qu'un tiers de confiance soit chargé de tenir à jour les équilibres de chaque utilisateur. En revanche, ces systèmes créent peu à peu des poussières de comptes, qui peuvent être encombrants pour le réseau. Ethereum a su dépasser ce système, tout en ne recréant par de tiers de confiance.

Traitements complexes

La gestion de l'état de l'ether diffère de celle du bitcoin ; en effet, elle permet de prévoir des actions futures à partir d'inscriptions passées, ce qui permet des traitements complexes, c'est-à-dire des opérations à plusieurs phases.

Diversité des applications

Ethereum présente une plus grande diversité d'applications que Bitcoin. Cela s'explique par son API de plus haut niveau, c'est-à-dire que son langage de programmation est plus richement fourni. Cela signifie que les programmeurs peuvent plus facilement développer des applications puissantes.

Cela s'explique aussi par son infrastructure, avec l'utilisation d'ENS qui sont des adresses Ethereum comparables aux adresses DNS du web, et Swarm, qui est une application de partage de documents décentralisés, utilisant des incitations économiques pour fonctionner.

Ces composants font d'Ethereum une plateforme permettant de porter des applications diverses, dépassant le simple usage de gestion et de transfert de valeur auquel semblent parfois cantonnées les *blockchains* publiques.

Les traitements sur la *blockchain* Ethereum ont, en général, une valeur ajoutée, ou permettent de créer de la valeur. La dernière application à très grand succès d'Ethereum fut l'application de divertissement « crypto-kitties » consistant à acheter et échanger des chats virtuels uniques inscrits sur la *blockchain*. Dépassant en termes de bénéfices les plus importantes levées de fond en cryptomonnaies (*Initial Coin Offering, ICO*), ce succès met en lumière la subjectivité de cette valeur ajoutée.

Proofs of stake

Il y a en réalité deux « *proofs of stake* » : la preuve de détention et la preuve d'enjeu, qui sont décrites en anglais sous le même terme alors qu'elles sont assez différentes dans leur fonctionnement et leurs intérêts.

La **preuve de détention** est utilisée par les cryptomonnaies NXT, Blackcoin ou Peercoin. Il s'agit d'attribuer le droit de valider un bloc (équivalent du minage, sans avoir à fournir de preuve de travail) de manière aléatoire, en attribuant plus de chances aux plus importants détenteurs de cryptomonnaies.

On l'appelle aussi *proof of stake* naïve car il n'y a pas de pénalité en cas de fraude de la part du mineur désigné, pas d'enjeu. On dit qu'elles sont donc susceptibles d'attaques par *« nothing at stake »*. Les protocoles tels que *Proof of Capacity* ou *Proof of Activity* sont similaires car ils consistent toujours à prouver que l'on dispose de quelque chose.

La **preuve d'enjeu** pondère l'attribution aléatoire du droit de valider un bloc en fonction d'un nombre de cryptomonnaies mises en séquestre par les « mineurs », ils peuvent donc être pénalisés en cas de démarche frauduleuse.

Le protocole *Slasher* (Vitalik Buterin) implémente ainsi des pénalités pour les créateurs de blocs sur les branches validées par d'autres validateurs. L'enjeu sera « brûlé » en l'envoyant à une adresse dont personne ne possède la clé privée.

Ce mode de preuve permet le *sharding*, c'est-à-dire la fragmentation de la *blockchain* qui, contrairement aux systèmes utilisant la preuve de travail, permet la montée à l'échelle (*scalability*). Par ailleurs, personne n'est pénalisé s'il travaille sur la mauvaise branche.

Le risque de collusion ploutocratique reste toutefois très important, des validateurs disposant d'une énorme somme pourraient se coaliser pour attaquer la chaîne. C'est une des raisons pour laquelle le passage à la *proof of stake* sur Ethereum prend du temps, de nombreux tests sont nécessaires. Ce risque se vérifie toutefois aussi pour les systèmes de *proof of work* avec la coalition des fermes de minage.

La ***proof of stake* déléguée** (DPoS) ne fonctionne pas bien, c'est le système utilisé par les cryptomonnaies *Dash*, *Steem* ou *EOS*. Il consiste à avoir peu de validateurs effectifs, appelés « masternodes » qui sont « élus » par les autres nœuds du réseau. Si en théorie le système est démocratique, il se révèle ploutocratique dans la réalité. En mars 2018, il a vu une « guerre » entre validateurs chinois et américains dans une chasse aux votes pour obtenir les délégations.

Ripple

Ripple est une monnaie centralisée qui a l'avantage de proposer un très grand nombre de transactions par secondes. En revanche, ce nom recouvre deux activités dissociées : une *blockchain* privée bancaire, très efficace, et la monnaie XRP, qui présente une très forte capitalisation et est « pré-minée », donc pas réellement décentralisée.

Ses gestionnaires jouent sur l'amalgame entre ces deux activités, ce qui en fait une cryptomonnaie très impopulaire dans l'écosystème *blockchain*.

Couches de niveau 2

Les couches supérieures sont distinctes du réseau principal et permettent de réaliser des transactions plus rapidement et avec beaucoup moins de frais. Pour le bitcoin, on parle des *lightning networks* qui sont envisagés pour les micro-paiements ; il s'agit d'enregistrer la trace de paiement sur la *blockchain*, sans y inscrire l'ensemble de la transaction. Sur Bitcoin, la pérennité du système est discutable car il reste avant tout une réserve de valeur.

Ethereum, en plus du *sharding* qui permet de travailler sur plusieurs branches en même temps, propose plusieurs réseaux secondaires. *Raiden* fonctionne tant que peu de personnes ne l'utilisent, mais des solutions pourraient être trouvées pour sa montée en puissance.

Les *State Channels* sont encore en développement, comme *Truebit* qui permet de l'exécution de code hors chaîne.

Plasma, une solution externe à Ethereum, peut y servir comme couche de deuxième niveau ; c'est une solution notamment utilisée pour les webcammeuses, *Plasma cash* en est un dérivé encore en développement.

L'activité des webcammeuses est un cas d'usage marquant car leurs rémunérations aux USA sont bloquées par PayPal, pour des raisons de puritanisme.

Méta-protocole et ICO

Il s'agit d'une levée de fond reposant sur une forme d'abstraction économique : les *tokens* (jetons). Parmi les ICO, il y a beaucoup d'arnaques, près de 99 % de projets inutiles ou excessifs. De manière générale, dans le monde des cryptomonnaies, il y a beaucoup d'arnaques, le site *CryptoFR* en recense un certain nombre. Le régulateur devrait s'emparer plus sérieusement de la question.

Consommation électrique

On peut estimer la consommation du bitcoin autour de 15 TWh/an. Il s'agit surtout d'une électricité peu chère provenant de barrages chinois inutilisés ou de la géothermie en Irlande, le reste provenant effectivement de combustible fossile.

Il faut mettre le coût de minage du bitcoin en comparaison avec l'exploitation d'aluminium et d'or, avec la dépense énergétique de climatisation immobilière ou encore avec la consommation de sites comme Facebook, dont on peut questionner l'utilité sociale.

Les déterminants de la consommation énergétique semblent corrélés à la part du *hashrate* de chaque monnaie par rapport aux autres monnaies. Cela s'est notamment vu lors de la création d'Ethereum Classic.

Pour réduire la consommation d'Ethereum, l'utilisation de systèmes de consensus alternatifs est la piste la plus probante. Dès l'origine, Vitalik Buterin voulait se séparer la preuve de travail pour éviter le gaspillage et par méfiance pour les mineurs. Le protocole *Casper* vise à implémenter la *proof of stake* pour Ethereum, il est encore en test car des milliards étant en jeu, les développeurs n'ont aucun droit à l'erreur.

Pour Jean Zundel, la nécessité d'un sous-jacent énergétique est une chimère, il soutient en effet que certaines monnaies classiques ont perdu leur sous-jacent physique (les pièces ne sont plus en or ni en argent) sans que le système ne cesse de fonctionner.

Pour la sécurité, le nombre de mineurs est essentiel, plus il y en a, plus il y a de sécurité. Dans le milieu des cryptomonnaies « il est prudent d'être paranoïaque ».

Solutions alternatives aux blockchains classiques

Les DAG (*Directed Acyclyc Graphs*) sont des registres distribués qui forment des graphs plutôt que des chaînes, un bloc pouvant être suivi ou précédé par plus d'un autre bloc. Toutefois, l'ensemble du graph a une même direction, c'est-à-dire qu'en suivant un chemin de bloc en bloc on ne peut revenir deux fois sur le même.

Les transactions, par exemple les informations d'une caméra, sont validées par seulement deux pairs qui eux-mêmes veulent valider une transaction. Cela signifie que tout le monde est mineur.

Le système *Tangle* de IOTA, qui utilise un DAG, constitue « une arnaque à caractère sectaire », ses promoteurs ne sont pas dignes de confiance.

Bien moins connu, *Byteball* est fonctionnel et plus complet.

Le système *Hashgraph* ressemble à un DAG mais Jean Zundel n'a pas vraiment eu l'occasion de l'étudier. Il semble très rapide en environnement fermé (*permissioned*) et utilise un algorithme de consensus byzantin en environnement asynchrone. Tous ces DAG ne sont pas

adoptés, la sécurité n'a pas été réellement testée sur un réseau massif. Il faut que ça devienne assez intéressant pour qu'on se mette à l'attaquer.

Identité et autres usages d'intérêt

Les principes de la *blockchain* et du droit à l'oubli sont incompatibles, une *blockchain* n'est pas faite pour gérer des secrets.

Cependant, il y a des pistes, à un niveau très expérimental, pour garantir la confidentialité. C'est ce que l'on appelle le *zero knowledge proof*, développé par Zcash et intégré dans Ethereum, cette fonctionnalité reste toutefois inusitée. Cette technique permet de prouver des informations sur un émetteur de données sans dévoiler le contenu de ces données, par exemple son âge ou sa nationalité. Le principe est de construire une preuve intégrée à la chaîne, comparable à une signature mais bien plus complexe.

La *self-sovereign identity*, identité auto-souveraine, revient à permettre à une personne de définir elle-même sa propre identité numérique et d'en maîtriser tous les tenants et aboutissants. Il serait intéressant de créer un lien entre cette identité et l'identité réelle.

Le secteur de l'économie sociale est intéressant car une *blockchain* permet de collecter des contributions et de redistribuer les fonds avec des règles complexes en toute transparence. C'est l'ambition du projet *DAO 1901*, par exemple.

Ces solutions supposent de gérer correctement la protection de l'identité. De ce point de vue, le saut quantique est une menace qui apparaît encore lointaine.

Blockchain souveraine

Créer une *blockchain* souveraine semble inutile. Si le problème venait à se poser, il faudrait se demander pour quoi faire, avec quels acteurs et quel problème de théorie des jeux à résoudre. Les projets existants ou ayant existé fonctionnent mal ou ont mal fonctionné (Auroracoin en Islande, Francs.paris, Cryptogaule, Paypite pour la francophonie…), les cryptomonnaies sont transnationales par nature.

Conclusion

La France possède des compétences fortes en matière de *blockchain*, en particulier des cryptographes parmi les meilleurs au monde. On note toutefois qu'il n'y a pas de plateforme d'échange française. Il faut consulter les leaders du marché pour connaître leurs besoins.

Enfin, il faut à la fois sortir du mythe de la *blockchain* sans cryptomonnaie, et lutter contre les nombreuses arnaques.

2. MM. Ken Timsit, directeur général de Consensys France et Jérôme de Tychey, responsable *blockchain* chez Consensys et président de l'association Asseth

La technologie *blockchain* est convaincante en ce qu'elle amène de nouvelles manières de travailler. Elle n'est pas faite à l'origine pour faire uniquement des ICO (levées de fond) et peut avoir un grand nombre d'autres applications.

Ethereum fonctionne grâce à environ 30 000 serveurs en réseau qui utilisent des jetons appelés ethers qui sont une incitation au fonctionnement en réseau pair à pair à grande échelle. En effet, utiliser une cryptomonnaie est ce qui permet de créer des effets réseau.

Il est important de comprendre qu'Ethereum est à la fois **un protocole** et **une *blockchain* publique**. En effet, sa technologie peut être utilisée pour des *blockchains* privées, ou des *blockchains* « de consortium ». C'est par exemple le cas de la *blockchain Quorum* développée par Consensys avec la banque JP Morgan.

Les principaux cas d'usages peuvent être regroupés en quatre catégories, pour ce qui est des activités de Consensys :

- la **supply chain** pour la traçabilité (bœuf, pétrole, titres de propriété, thon…) ;

- les **services financiers**, où la *blockchain* sert par exemple pour auditer les *KWC*, des titres financiers ;

- les **échanges énergétiques** : par exemple un distributeur d'électricité du Texas utilise la *blockchain* pour certifier l'énergie produite et reçue par ses clients et fournisseurs ;

- dernier cas d'usage : **gérer l'identité sur la *blockchain***. Les protocoles d'échange de données sur lesquels travaillent Consensys permettent de rendre ces données portables. Cela permet de faire des authentifications où la personne peut accéder à des applications en étant pleinement possesseur de ses données.

Il est possible de monter des projets interopérables entre Ethereum et Bitcoin (ex : BTC-relay).

En matière de gestion de l'identité par exemple, il est nécessaire qu'il y ait un tiers de confiance pour certifier une caractéristique d'un utilisateur (son âge, sa nationalité…) mais ce tiers est totalement remplaçable, il n'a pas le monopole de la certification.

La plupart des applications de Consensys sont d'abord développées sur une *blockchain* privée puis éventuellement mises en œuvre sur la *blockchain* publique.

Pour Ken Timsit, on ne peut pas dissocier les deux et peu à peu les deux vont se développer de manière conjointe. Pour beaucoup de systèmes un niveau de consensus moindre est nécessaire. Plusieurs *blockchains* publiques centrales se verront connectées à des *blockchains* privées.

Celles-ci publieront régulièrement leurs résultats sur ces *blockchains* publiques, il sera donc possible d'y retrouver un état sécurisé donné à un moment donné en cas de contestation des résultats (tous les jours, toutes les semaines...).

Ronan Le Gleut : La *blockchain* Ethereum n'est-elle pas appelée à être dépassée par une nouvelle technologie, plus performante? Dans ce contexte, pour une entreprise ou une institution, faut-il miser tous ses œufs dans le même panier en ne se fondant que sur les solutions d'une seule *blockchain* ?

Ken Timsit et Jérôme de Tychey : Aujourd'hui, Ethereum est très largement dominant en termes de transactions avec 80 % des transactions échangées ainsi qu'en nombre de développeurs, puisqu'il représente 80 % de la communauté de développeurs sur *blockchain* dans le monde.

Ethereum est dans une situation similaire à ce que fut celle d'Android, qui était un système basique faiblement développé sur lequel des acteurs extérieurs ont installé des applications. En observant le fonctionnement et/ou les dysfonctionnements de ces applications, Android a pu développer de nouvelles applications plus performantes. Pour

Ethereum ce fut le cas par exemple de Zcash et de Monero, qui ont vu leurs technologies d'offuscation très rapidement copiées sur Ethereum.

Cela dit, comme pour tout projet de start-up, le risque de se voir dépassé subsiste.

Avantage comparatif de l'utilisation d'une solution blockchain

Ethereum a un cahier des charges qui lui permet d'avoir plusieurs clients, c'est-à-dire plusieurs « interfaces », adaptées aux applications souhaitées. On peut faire un parallèle avec les navigateurs internet, qui sont divers mais permettent tous de naviguer sur le web.

Le principal intérêt de la *blockchain* c'est la scalabilité, c'est-à-dire la possibilité d'avoir un très grand nombre d'acteurs en consensus, facilement. Plus les acteurs sont hétérogènes et nombreux, plus on aura besoin de traçabilité et donc de *blockchain*.

Ce consensus se fait différemment en *blockchain* que dans d'autres solutions, car il suffit de lire le code pour l'auditer.

Passage à la proof of stake

La *proof of stake* permet le passage à l'échelle et de faire du *sharding*, c'est-à-dire de miner sur plusieurs branches. Pour s'assurer qu'il y a un consensus large sur le dernier le bloc, la *proof of work* propose une sécurité économique, c'est-à-dire sur la quantité d'argent nécessaire à résoudre le hash. Avec la *proof of stake*, il y a aussi une sécurité économique car les gens mettent en jeu leurs ethers.

L'idée du protocole CASPER, qui veut implémenter la *proof of stake* dans Ethereum, c'est d'exiger un certain nombre de signatures sur un bloc pour qu'il soit considéré valide. La difficulté à attaquer ce système est liée à la surface d'attaque, c'est-à-dire à la taille et à la dispersion du réseau. CASPER est un algorithme de sanction, qui permet d'être résilient en cas d'attaque.

Il faut noter que Consensys utilise différents algorithmes de consensus selon les types d'application.

Observatoire européen de la blockchain

L'objectif de la Commission européenne avec cet observatoire, c'est de ne pas rater le train comme ce fut le cas avec internet. Il s'agit de faire fructifier l'activité d'innovation autour de la *blockchain* en Suisse, en Allemagne, en France et dans une partie de l'Europe de l'Est.

Trois axes sont donnés à cet observatoire, dont Consensys a remporté l'appel d'offre public :

- développement d'un site éducatif sur la *blockchain* ;

- constitution d'une « *framework* » réglementaire à proposer aux pays membres ;

- réflexion sur des applications *blockchains* au niveau gouvernemental sur lesquelles on pourrait lancer des projets européens.

Valéria Faure-Muntian : Comment expliquer qu'une compagnie américaine ait été choisie par l'Union européenne pour orienter sa politique, surtout s'il y a des compétences en Europe ?

Ken Timsit : L'appel d'offre a été remporté par une association, l'université de Lucerne et deux universités anglaises. Par ailleurs, Consensys possède des bureaux à Bucarest, Berlin ou Paris. Les rapports seront publics, de manière générale 90 % des productions de Consensys sont en open-source sous licence GPLv3 (réutilisation autorisée sans but commercial).

3. MM. Nicolas Courtois, professeur à l'University College of London, Vincent Danos, chercheur au département d'informatique de l'École Normale Supérieure et Daniel Augot, chercheur à l'INRIA

Nicolas Courtois : La plupart des *blockchains* ne sont pas assez sécurisées. En effet, en cryptographie, plus il y a d'argent en jeu dans un système informatique donné, plus il va être exposé.

Les *blockchains* les plus populaires ou les plus commercialisées, au premier rang desquelles celle du bitcoin, ne sont pas forcément les plus abouties, c'est une autre règle que l'on retrouve souvent en informatique. Il y a beaucoup de cas où la mauvaise technologie est répandue et où la bonne n'est jamais utilisée. Très souvent, les ingénieurs n'arrivent pas à faire passer leurs idées pour sécuriser les systèmes.

Il y a une stratégie industrielle qui consiste à utiliser une cryptographie différente pour les bitcoins ou les ethers de celle qui est classiquement utilisée dans des projets reconnus au niveau académique. Les communautés de développeurs sont assez fermées et se situent en dehors des réseaux académiques. Beaucoup de ses développeurs arrivent par effet d'aubaine et plusieurs sont malhonnêtes, la plupart ne sont pas indépendants mais travaillent pour des entreprises comme Consensys.

Critiques du Bitcoin

- Il est faux de croire que l'on peut facilement réduire la consommation énergétique sur la *blockchain*.

- Le bitcoin est utilisé massivement par de nouveaux criminels, par exemple pour du rançonnement, mais cette réalité a assez peu d'écho dans les médias.

- Si la technologie est suffisamment sûre à très court terme, rien ne permet d'affirmer que demain des millions de bitcoins ne partiront pas en fumée. Pour prévenir une attaque, il est certes possible de faire un *fork* mais c'est très rare et surtout contraire à l'éthique de la mouvance à l'origine du bitcoin.

- Le système de Nakamoto a été dévié de son utilité originelle. D'un système soi-disant anarchique et démocratique, il est passé à un système où seuls les plus gros ont pu concevoir leurs propres machines de hashage, en masse. Beaucoup d'argent a été perdu par les petits « actionnaires » du bitcoin.

Le bitcoin utilise aujourd'hui SHA-256, qui est très efficace mais qui devrait être cassé un jour, d'ici 20 ans selon Nicolas Courtois, plutôt d'ici 100 ans pour Daniel Augot.

En ce qui concerne la signature, si l'on voulait changer aujourd'hui les courbes elliptiques de Bitcoin, cela serait complexe à cause de l'inertie de la communauté. Pourtant, la

NSA s'est détournée de la cryptographie à courbes elliptiques en 2018, après l'avoir imposée en 2004. En effet, celle-ci sera mise à mal par l'informatique quantique.

La cryptographie universitaire et les techniques non académiques

Jusqu'à très récemment il n'y avait aucun cryptologue dans les principales communautés *blockchain* comme celles de Bitcoin ou d'Ethereum… La plupart de leurs membres sont des autodidactes, qui ne sont pas au fait des travaux universitaires.

Cela peut s'expliquer en ce que de nouvelles formes d'organisation de l'investissement émergent. Si on applique les grilles de lecture universitaires et économiques standards, les résultats apparaissent complètement anormaux, mais cela ne veut pas dire que ça ne fonctionne pas.

Ce qui est intéressant avec le succès du bitcoin, c'est qu'une innovation technologique née en dehors de la sphère universitaire a remporté un large succès. Les universitaires se retrouvent donc dans le rôle inverse d'étudier un objet pratique pour en tirer les règles théoriques. Sous l'effet de la « vague » *blockchain*, les scientifiques se réattaquent à des questions anciennes qu'ils avaient délaissées, comme le consensus byzantin ou les algorithmes de consensus.

Smart contracts

Il y a beaucoup de naïveté concernant les *smart contracts*, qui ont des modèles faiblement résistants. Une des principales erreurs consiste à penser que l'on peut auditer le code simplement en le lisant. Or, en programmation, beaucoup d'erreurs sont contre-intuitives. Les techniques utilisées pour vérifier les logiciels critiques, dont Bitcoin fait partie, impliquent une vérification expérimentale du code avec de nombreux tests.

Ainsi, l'équipe de Vincent Danos vérifie-t-elle que les codes sont corrects en réalisant des tests automatisés, puis en établissant des modèles mathématiques permettant ou non de prouver la sécurité contre un type d'attaque donnée. Pour le bitcoin on retrouve quelques erreurs graves.

Il revient ensuite sur l'histoire de *TheDAO*. La communauté a décidé de modifier la machine pour empêcher l'attaquant d'en jouir.

Alternatives

Le cryptographe très réputé Silvio Micali a créé la *blockchain* Algorand, dont la théorie sur le papier semble très sûre. Il a déposé une quinzaine de brevets (ce qui aura cependant pour effet de verrouiller la recherche publique).

Cependant, si la technologie est sûre, cela ne signifie pas qu'elle va emporter un réel succès. Il y a un marché de l'effort de développement sur certaines solutions et énormément de volatilité sur le type de technologies qui va gagner.

La sécurité restant forcément liée à une incitation économique, le problème d'Algorand reste que l'on suppose au moins un tiers de nœuds bienveillants pour que le système fonctionne, il y a un risque de multiplication d'identités.

Sécurité

Vouloir un système 100 % sécurisé est un peu illusoire, en réalité, un système est sécurisé par rapport à une attaque maximale envisagée : qui est l'adversaire et quels sont ses moyens ?

Il existe deux niveaux de risque pour le bitcoin : cryptographique, avec un cassage du cryptage, et opérationnel, avec une coupure du réseau, un vol de mot de passe, ou encore « l'encerclement » d'un nœud. Il a ainsi été démontré qu'il est possible d'isoler artificiellement un nœud en corrompant tous les nœuds l'entourant pour lui donner de fausses informations, une fausse évolution du registre.

Pour **Nicolas Courtois**, beaucoup de problèmes sont liés au manque de responsabilité des codeurs, dans le monde du logiciel personne n'est sanctionné si un bug est créé.

Objectifs et fonctionnement de la blockchain

Vincent Danos : La *blockchain* présente une transition dans la manière de conduire des affaires, c'est une architecture de la confiance. Il s'agit de produire de la confiance à moindre coût en diminuant la corruption, le gâchis, les frictions ou encore les coûts cachés, ce que Vincent Danos appelle la « *trust tax* ».

Le but de la *blockchain* est de réduire la *trust tax,* car plus il y a de besoins de confiance, plus il y a de coûts prudentiels. Si la confiance est plus simple à obtenir, les contrats sont plus rapides, voire automatiques. Tout l'enjeu est de trouver une solution où les différents acteurs ne pourront pas se fédérer pour biaiser les décisions, mais où ils pourront tout de même se mettre d'accord sur une version de la vérité.

Comme pour le vote, le bon fonctionnement du mécanisme implique une quantité de processus très subtils auxquels on ne pense pas. Par exemple, il n'est pas possible de prendre tous les bulletins de vote dans l'isoloir pour ne pas pouvoir prouver que quelqu'un n'a pas voté pour quelqu'un d'autre.

Pour lutter contre les fraudes (dans le cas du bitcoin, une double dépense), on peut soit agir en aval lorsqu'on la constate, soit s'assurer avant l'écriture du bloc que la fraude n'est pas possible (algorithme byzantin), soit s'assurer après l'écriture du bloc que celui-ci est bien valide, et l'accepter ou le refuser le cas échéant (c'est le fonctionnement du bitcoin).

À noter qu'il ne faut pas confondre l'embranchement de deux blocs (*possible double-spending*) et le fait de laisser passer des transactions invalides, la validation n'est pas la même chose que l'inscription.

Il faut pouvoir s'assurer d'intéresser les gens au système, à être assesseurs pour continuer le parallèle avec le vote, en sachant qu'il ne faut pas qu'ils soient de la même couleur politique. L'idée ici est de les payer en les récompensant avec des paiements non susceptibles de corruption : en cryptomonnaies.

Confidentialité vs audatibilité

Il y a une tension entre l'exigence de vérifiabilité par tous et celle de confidentialité des échanges. Les méthodes *zero knowledge* visent à répondre à cette tension grâce à des

méthodes cryptographiques ; il est possible de gérer des actions sans obliger qu'elles s'affichent toutes en clair.

Initial Coin Offerings

Pour **Vincent Danos**, le véritable nouvel objet émergent est l'ICO, des levées de fonds où les investisseurs reçoivent des *tokens*, auxquels sont attachés des propriétés ou des droits d'usage liés au développement futur des produits. Ces *tokens* peuvent être revendus et échangés sur un marché secondaire.

Le phénomène est considérable, les ICO constituaient 10 % des levées de fond au monde en 2017. C'est un mécanisme très intéressant et il y a des recherches économico-informatiques en cours sur le sujet.

Daniel Augot : L'introduction du papier de Nakamoto contient un exergue politico-philosophique, l'idée étant dès le départ de se séparer du tiers de confiance. Il faut noter que le mot « *blockchain* » n'est pas utilisé dans le document de Nakamoto.

Le principe du registre horodaté ne date pas d'hier, la particularité du bitcoin vient de son relatif pseudonymat, où il n'y a pas d'officier signataire mais un mineur. En revanche, la notion d'horodatage est toujours présente.

Doit-on s'interroger sur les différences entre les technologies « *blockchain* » et les avantages et inconvénients des différents modes de consensus, ainsi que sur les technologies alternatives de registre distribué ?

C'est un sujet si complexe que ce pourrait être un sujet de thèse. Pour parler des avantages et inconvénients des différentes cryptomonnaies, il est nécessaire d'aller plus loin que les seules questions de consensus.

Que signifie « distribué » ? Côté utilisateur, s'interroger sur l'ouverture, qui peut participer au réseau ? Côté système, qui maintient le registre et valide les écrits ?

Y-a-t-il un enregistrement préalable/dynamique des entités de validation ou une ouverture à tous en tout temps ? Qui décide des règles et de leur évolution ?

Les différentes technologies (PoW, PoS, PBFT…) permettent toutes de réaliser les fonctionnalités de « *ledger* » demandées par le public, c'est-à-dire l'immuabilité et la sécurité. Les considérations techniques lui sont difficilement accessibles, la transparence doit porter sur ces deux critères mais les utilisateurs n'auront pas forcément à savoir comment quel type de protocole fonctionne.

Les seules différences perceptibles par l'utilisateur porteront sur la performance, les coûts, la protection de la vie privée, la confiance, l'adhésion à la gouvernance… comme pour un service financier, bancaire ou notarial, sans se soucier de la technologie.

Sécurité

Aujourd'hui encore, la force de la *blockchain* c'est la fonction de hash, SHA-256 pourra durer encore 100 ans pour l'usage qui en est fait ici.

Pour beaucoup de ces projets, la sécurité est fondée sur la rationalité des acteurs, qui ne feraient pas une action qui déprécierait la valeur des cryptomonnaies qu'ils acquerraient par exemple. Avant de parler de chiffrement, il faut décider de quoi veut-on que

le système soit sûr : de la majorité de quoi ? Le cryptographe ne peut ni se dire que la majorité est honnête, ni nier l'hypothèse qu'un « fou » soit prêt à perdre de l'argent pour voir le réseau crasher, c'est l'attaque *Goldfinger*. Le 25 mai au matin, il y a eu une attaque 51 % sur Bitcoin gold.

Daniel Augot est en désaccord avec Nicolas Courtois sur la possibilité de voler ou modifier le code source sans que quiconque s'en aperçoive. Il estime en effet le système protégé par la masse. Il est possible de faire l'analogie avec les billets de banque qui peuvent être volés, ce qui est dommageable à leur propriétaire, mais pas à la banque centrale, qui y survit.

Proof of stake et autres alternatives

Dans la *proof of stake*, chaque personne qui a pu obtenir des cryptomonnaies a une part. Une personne va être tirée au hasard et va signer un bloc, elle pourra être récompensée ou non. La rapidité d'exécution et la faible consommation d'énergie sont les gros arguments de vente de la *proof of stake*. La consommation énergétique est sans équivoque le point noir du bitcoin.

Remarque de Vincent Danos : il est à noter que puisque les ratios sont conservés, la part de chacun augmente de manière égale car chacun voit son actif augmenter proportionnellement à la même vitesse, il n'y a donc pas de risque de capitalisation par un acteur.

Dans la *proof of work*, le mécanisme de récompense a un prix fixé, mais dans la pratique chacun l'indique dans son bloc puisque c'est de la monnaie créée *ex nihilo*. Si le créateur l'augmente artificiellement (par exemple en s'attribuant 13 BTC au lieu de 12,5), le reste du réseau va refuser d'ajouter ce nouveau bloc. Un membre du réseau qui serait majoritaire pourrait donc augmenter sa récompense et valider ses propres blocs ainsi créés.

Daniel Augot croyait assez peu à la *proof of stake* mais des papiers comme celui de *Cardano* semblent finalement assez solides. L'idée est d'organiser un protocole de vote virtuel qui ne demande pas de ressources.

Concernant le test du projet *CASPER* d'Ethereum, il faut comprendre que dans la culture scientifique, tester ne signifie pas apporter des preuves mathématiques, c'est-à-dire des preuves de non-existence de failles. Pour *Cardano* il y a une démonstration mathématique de la sécurité, pour un nombre minimal donné de personnes non-malveillantes.

La *proof of useful work* est un projet, aujourd'hui en sommeil, consistant à utiliser la puissance informatique nécessaire au minage à des fins utiles, comme par exemple la modélisation complexe de molécules en 3D.

Il faut bien distinguer :

- la *proof of work*, dont le fonctionnement est bien compris ;

- la *proof of stake*, encore à l'état expérimental ;

- les algorithmes classiques de consensus (PBFT, RedBelly, tendermint), qui bénéficient de trois décennies de recherche, sont bien compris mais ne sont utilisables que dans des modes *permissioned*, où les acteurs sont connus ou contrôlés.

Les DAG comme IOTA sont très discutables, il faut savoir sur quoi porte le consensus. Ils ne sont aujourd'hui pas sûrs du tout car il est facile de faire dérailler un « fil » du graph, la sécurité du système se partageant en autant de parts que de fils.

Autres utilisations de bitcoin

Le bitcoin pourrait potentiellement rendre beaucoup plus de services, par exemple proposer le contrôle d'un stockage distribué grâce à sa capacité d'horodatage. Il pourrait servir à certifier un grand nombre de données, grâce notamment à la fonction *OP-Return*, qui permet d'insérer 256 bits de caractères libres en plus d'une transaction (c'est-à-dire un hash).

Le *lightning network*, très prometteur, permet des micro-transactions.

Le bitcoin est programmable, on peut y mettre les monnaies sous séquestre pour qu'elles soient délivrées à certaines conditions, c'est l'origine des *smart contracts*. Il est possible de fluidifier les transactions en inscrivant seulement un solde de tout compte, un *merkle root*, d'un grand nombre de transactions.

C'est ce que fait la société française *Acql*. Une autre entreprise, travaillant sur l'identité biométrique, avait besoin d'une garantie pour stocker ses données et s'est intéressée au bitcoin car c'est une solution très peu chère.

Les enjeux juridiques

Une doctorante en droit, Hanna-Mae Bisserier, travaille au quotidien dans l'environnement du projet BART, ce qui lui donne un regard particulier. Pour elle, ces technologies créent un régime particulier « conventionnel et technique ».

Le droit à l'oubli est fondamentalement opposé à la fonction de registre. Cependant, l'anonymat pourra être garanti, des solutions techniques existent.

Souveraineté

La *blockchain Duniter* n'est pas très sérieuse scientifiquement mais originale politiquement, portée dans les milieux altermondialistes. L'idée est d'éliminer la preuve de travail avec un don universel d'une part de la monnaie à chaque nouvel arrivant. La masse monétaire croit donc avec les nouveaux arrivants. Il y aurait aussi une réflexion à la Mairie de Paris autour d'une monnaie locale *blockchain*.

V. AUDITIONS DU 29 MAI 2018

1. MM. Renaud Roquebert, avocat conseil et Bilal Chouli, co-fondateur de Neurochain

Renaud Roquebert est avocat en nouvelles technologies, il a vécu dans la Silicon Valley et s'est beaucoup intéressé aux problématiques fiscales et réglementaires des *blockchains*. Il accompagne le projet Neurochain. Selon lui, les problématiques fiscales et réglementaires sont probablement le principal frein au développement des *blockchains*. Il y aurait beaucoup d'annonces gouvernementales mais peu de réalisations opérationnelles.

Bilal Chouli a travaillé et étudié au CEA, à Oxford et à Polytechnique. Après son doctorat il a bifurqué vers la finance quantitative, puis l'intelligence artificielle.

Assez tôt, il a écrit un livre sur les systèmes distribués. Aujourd'hui, il a cofondé Neurochain, un projet scientifique, avec une nouvelle plateforme *blockchain*.

Neurochain et Initial Coin Offerings

La société a été créée en deux temps, d'abord sur fonds propres puis au terme d'une *Initial Coin Offering*, l'industrialisation est aujourd'hui prête.

S'ils ont procédé à une ICO, c'est d'abord car le produit « Neurochain » est *open source*, la technologie est disponible pour tous, donc la société qui porte la technologie n'a pas intrinsèquement de valeur, en être actionnaire n'est pas très intéressant. Par ailleurs, l'ICO permet de toucher immédiatement une plus large communauté sur des projets dont la compréhension demande un fort bagage scientifico-technique ; les investisseurs classiques considèrent souvent ces projets trop incompréhensibles « *deep-tech* ».

Enfin, une levée de fond classique en France prendrait entre six mois et un an. Or, dans un environnement très rapide et de haute concurrence, il faut pouvoir lever des fonds rapidement.

En France, le phénomène des ICO reste mineur, elles sont principalement menées par des sociétés commerciales de type SA ou SAS. La société vend des « jetons » (*tokens*), qui juridiquement peuvent représenter un service en l'état futur d'achèvement, et comptablement un produit constaté d'avance. Mais c'est aussi un actif numérique car la plupart des achats ont été faits en crypto-actifs, principalement Ethereum.

Un des enjeux est de pouvoir convertir ces crypto-actifs en euros, sur des places de marché telles que *Kraken*, en Allemagne. Le FMI considère les cryptomonnaies comme un élément de la finance mondiale.

Cependant, aujourd'hui, les banques françaises refusent d'ouvrir des comptes à des sociétés qui ont fait des ICO, arguant essentiellement d'un problème de conformité aux réglementations de blanchiment d'argent et de lutte contre le terrorisme. C'est un problème qui va obliger les compagnies qui ont fait ce type de levées de fond à se domicilier à l'étranger.

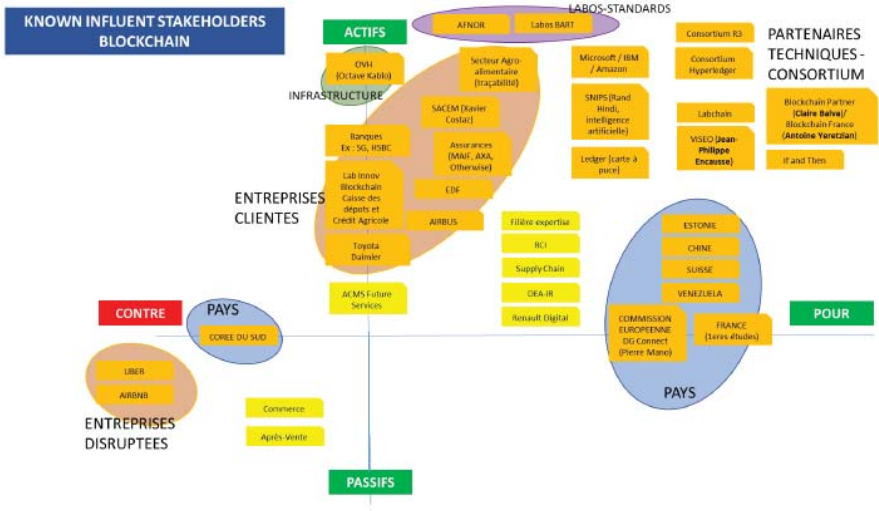
Définition des blockchains

La *blockchain* peut être définie d'un point de vue utilitariste comme une technologie qui permet un stockage, un transfert d'information, de valeur, de documents ou de données de manière directe, sans intermédiaire et automatisée. Les échanges et leur stockage sont immuables car enregistrés par les différentes parties constituées.

Il est aussi intéressant de considérer la *blockchain* d'un point de vue technique comme l'addition de trois composants bien connus depuis les années 80 : des algorithmes cryptographiques, des méthodes de consensus et un réseau.

Il faut bien distinguer les applications sur les *blockchains* des infrastructures de *blockchain*.

Panorama des acteurs



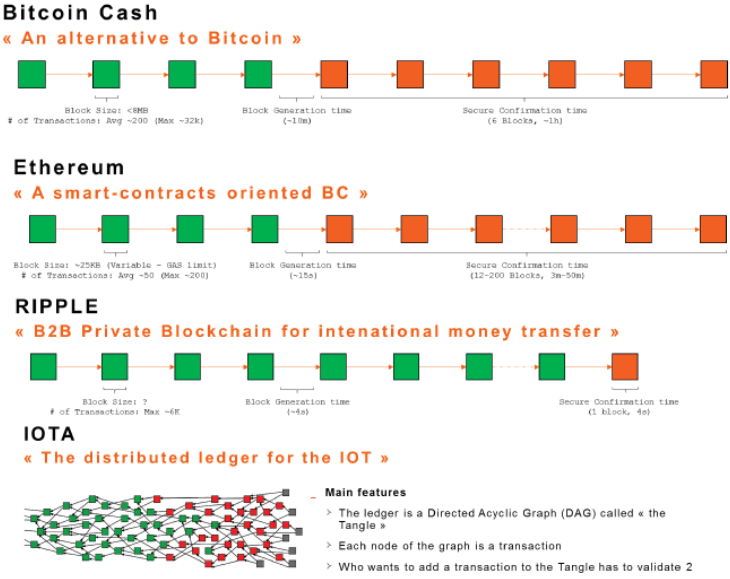
Source : Bilal Chouli

Beaucoup d'entreprises classiques ou des consortiums s'investissent pour la *blockchain*. En témoigne le protocole CORDA de R3, qui est un protocole d'échange sans cryptomonnaie sans consensus. Ici, la confiance est déportée vers les acteurs qui interagissent entre eux.

Pour un grand nombre d'applications, il n'y a effectivement pas besoin de consensus. Et pourtant, aujourd'hui, les projets sur la *blockchain* qui fonctionnent le mieux sont des projets business, qui améliorent sans réellement innover.

En France, il manque un leader politique qui porte la *blockchain* dans l'espace public et en fasse reconnaître les intérêts. Ainsi, des banques ont-elles pu reconnaître que le processus de validation des KWC, c'est-à-dire de contrôle des contributeurs à l'ICO de Neurochain, était beaucoup plus poussé que leurs processus actuels.

Si la France semble très favorable politiquement, elle a aussi des avantages concrets avec des ingénieurs loyaux, bien formés et parfois meilleurs que leurs concurrents américains.



Bitcoin Cash

Bitcoin Cash est un *fork* de bitcoin, il s'agit toujours de *proof of work*. Si ces protocoles fonctionnent c'est qu'il y a une économie parallèle du minage dont la rentabilité est colossale. En réalité, il n'y a pas beaucoup de transactions dans ces systèmes-là, c'est le minage qui fait leur richesse.

Ethereum

On peut attribuer aux différentes *blockchains* différents niveaux de maturité. Ainsi le bitcoin est très mature, fonctionnel depuis plus de 10 ans. Ethereum étant massivement développé et ayant repris beaucoup d'éléments du bitcoin, il a très vite atteint un niveau de maturité proche.

Ce protocole fonctionne toujours sous *proof of work* mais s'il y a une volonté de passer à la *proof of stake*, qui pose beaucoup de questions avec ce type de preuve, il n'y a pas de contrepartie physique.

Par ailleurs, du point de vue des mineurs, le passage d'un protocole pour lequel ils ont massivement investi à un autre où ils gagneront de l'argent de manière aléatoire n'est pas une bonne nouvelle. Il pourrait y avoir un refus d'adoption par une grande part du réseau.

Le problème de la rapidité pour une *blockchain* publique, c'est que des *forks* se créent plus facilement car il y a forcément une à vingt secondes de latence pour que le bloc se diffuse dans tout le réseau. La solution de Neurochain, pour une diffusion

rapide qui évite les *forks*, c'est de « nommer » une assemblée restreinte de validateurs, à intervalles réguliers.

Ripple et IOTA

Ripple est un protocole d'échange *peer to peer*, orienté finance et banque, qui n'est pas à proprement parler une *blockchain* mais plutôt un protocole d'échange. IOTA est un protocole orienté vers l'internet des objets (IoT) donc permettant beaucoup de transactions avec très peu de frais, c'est une technologie encore peu mature.

Dans IOTA, il n'y a pas une chaîne mais un graph, c'est-à-dire que chaque nœud communique avec un autre nœud. L'artifice technique derrière c'est de dire que pour valider une transaction, il faut en avoir validé deux autres.

Figure 45: Development timeline – where are we now?

Performance et consommations énergétiques

Des agents de la Banque de France auraient estimé qu'une transaction en bitcoin demande autant d'énergie que pour produire des billets pendant six mois. Par ailleurs, si Ethereum a une consommation plus faible par transaction, les transactions sont plus nombreuses car elles ont lieu toutes les 15 secondes. Cette consommation est exponentielle, cette année cela risque d'exploser plus encore car 2018 est l'année de déploiement des applications.

Si le réseau de minage d'Ethereum est plus distribué que celui de Bitcoin, il reste concentré en Chine. Par ailleurs aujourd'hui, Ethereum est probablement le premier client de Microsoft en termes de location de *cloud*.

La question importante consiste à savoir quel protocole l'emportera. Le projet Neurochain répondrait aux préoccupations environnementales et aux enjeux de concentration en Chine, aux USA et en Russie.

Si les Russes sont bien positionnés, c'est qu'ils ont d'abord des connaissances et du savoir-faire. Par ailleurs, Vladimir Poutine a récemment annoncé que la Russie

devrait devenir le deuxième pays au monde pour le minage. À terme, il envisage de créer une *blockchain* pour ses échanges, afin de se substituer au dollar.

Règlement général de protection des données

La *blockchain* peut répondre à certains enjeux réglementaires, notamment en permettant la traçabilité des données. L'étape ultime de la *blockchain* consiste en une gestion intelligente de la donnée.

L'enjeu de la protection des données est plus de savoir ce à quoi va servir votre donnée, que de protéger sa diffusion dans le réseau. Avec la *blockchain*, on est moins dans le droit à l'oubli que dans le droit de contrôler ce qui va être fait de cette donnée. Par exemple, dès aujourd'hui en matière d'interdit bancaire, on ne parle pas de la suppression de la donnée mais de son contrôle.

Souveraineté

L'Union européenne a lancé un observatoire de la *blockchain* délégué à un organisme par appel d'offre. Il s'agit de Consensys, société américaine, canadienne et russe, qui est le bras armé d'Ethereum. Il faut noter qu'à la candidature de Neurochain d'une part, et de Renaud Roquebert, d'autre part, la Commission a répondu trois mois plus tard par un simple mail.

La souveraineté c'est la création de la technologie et l'adoption d'une technologie portée par des principes. Aujourd'hui, les réglementations françaises de protection du consommateur sont extrêmement efficaces y compris dans le domaine de la *blockchain*. Ainsi pour l'ICO de Neurochain, le contrat de vente est soumis au droit des contrats et il est permis de se rétracter en 14 jours.

Le biais de Consensys risque par exemple de proposer la vision d'une « tokénisation » de l'économie, ce qui ne répond pas à la vision française de l'économie, de partage du savoir et de la société.

2. M. David Pointcheval, chercheur au CNRS, ENS/Université PSL – INRIA

Alternatives à la proof of work

Parmi les alternatives proposées, on peut noter que Georg Fuchsbauer propose la *proof of space*.

Incitation

Le gagnant voit son portemonnaie automatiquement alimenté, mais le gain tend à diminuer vers zéro, chaque transaction offre des frais de transaction au gagnant. David Pointcheval se demande quelle incitation offrir aux mineurs dans un système sans monnaie, par exemple pour faire consensus dans d'autres contextes d'application, comme garantir des contrats.

Cryptographie

Les techniques de cryptographie évoluent avec le temps, ce qui est normal. En ce qui concerne le chiffrement, il n'y a aucun moyen de préserver la confidentialité dans le temps. En revanche, pour ce qui est de la possession, on peut renouveler les algorithmes de hashage.

On ne peut donc pas faire une confiance infinie au système cryptographique pour préserver la confidentialité dans le temps, mais si l'on renouvelle régulièrement les fonctions de hachage, on peut préserver la possession.

Registres distribués

La validation d'une transaction doit être publique, afin que les nœuds puissent la contrôler. C'est le rôle des mineurs de contrôler la validité des transactions, c'est-à-dire l'équilibre entre les transactions entrantes et sortantes.

La probabilité qu'une transaction non valide passe dans un bloc reste négligeable car les mineurs n'y ont pas d'intérêt. Cette vérification se fait de manière automatique.

Dans un système de *proof of stake*, l'enjeu va être d'éviter les attaques Sybil, c'est-à-dire la multiplication des identités qui permettrait à un acteur d'accroître artificiellement son impact dans un système où une identité vaudrait une voix.

En revanche, si on est dans un cas d'usage où des personnes ne se font pas confiance mutuellement, mais où on en connaît le nombre, il y a des techniques qui permettent de faire un choix sans mécanisme de preuve. C'est l'utilité de la cryptographie distribuée à seuil, où il suffit qu'un certain nombre de nœuds sur le total utilisent leur clé privée pour qu'une transaction soit faite ou qu'une information soit révélée. C'est ce qui est utilisé en France pour le vote électronique, notamment.

On parle aussi de multi-signature ou de signature distribuée.

Confidentialité

Le bitcoin est souvent perçu comme anonyme, alors que ce n'est pas le cas. Les transactions sont publiquement associées à des portemonnaies, le système est donc pseudonyme.

Certaines techniques permettent des alternatives, telles que le *zero knowledge*, qui permet de faire des transactions chiffrées mais publiquement vérifiables. C'est une preuve cryptographique que ce qu'il y a à l'intérieur d'une transaction vérifie bien la propriété recherchée, sans révéler le contenu de celle-ci.

Le prix de cet anonymat c'est que cela prend beaucoup plus de temps de générer une transaction avec une preuve *zero knowledge*.

On peut vouloir lever l'anonymat dans certaines conditions, on parle alors de révocation. Au lieu, comme dans la *zero knowledge proof*, de ne pas créer de clé de déchiffrement, on va fournir une clé de déchiffrement à une personne ou à un groupe d'acteurs. Ils ne pourront lever l'anonymat que collectivement, ou avec une certaine proportion des clés.

Ainsi, lors du vote électronique, on chiffre le bulletin afin de prouver qu'il contient bien un vote, et pas plusieurs, mais sans révéler le contenu du vote. La clé du déchiffrement est distribuée parmi les membres du bureau de vote qui pourront lever la confidentialité sur tous les bulletins afin de connaître l'orientation des votes. Une personne seule ne peut lever la confidentialité.

Ces outils cryptographiques sont bien connus et parfaitement opérationnels.

Blockchain souveraine

Dans l'éventualité d'une *blockchain* souveraine, contrôlée par l'État, on pourrait envisager une liste connue d'autorités de confiance, avec un seuil raisonnable de validation des transactions. Selon le nombre d'acteurs en jeux, il ne sera pas forcément nécessaire de faire de la *blockchain*. Il peut suffire d'utiliser la cryptographie distribuée à seuil, ou la signature.

L'utilité d'une telle *blockchain* paraît donc très limitée, voire nulle.

En matière de souveraineté cependant, on peut relever que le bitcoin repose sur l'hypothèse d'une absence de collusion de 50 % de la puissance de calcul, mais 60 % de cette puissance se trouve actuellement en Chine. Tout le monde aurait intérêt à une répartition plus homogène sur le globe.

3. Mmes Amandine Jambert, ingénieur expert à la CNIL, Guilda Rostama, juriste et Tiphaine Havel, conseillère parlementaire

C'est la première audition de la CNIL sur le sujet des *blockchains*, une deuxième est prévue avec la mission Aubert le 21 juin.

La CNIL et le sujet blockchain

Les premières réflexions remontent à 18 mois, mais le sujet reste émergent au sein de la Commission. L'acte fondateur a consisté en une série d'articles, souvent des revues de rapports, sur le site du laboratoire d'innovation numérique de la CNIL (*LINC*) pour une première approche. Le dernier en date s'intitule « *Blockchain et RGPD, une union impossible ?* ».

Le sujet est désormais traité au sein de la direction des technologies et de l'innovation, au sein de laquelle un pôle fait un point de contact avec tout l'écosystème *start-up* et *innovation*. Un binôme, Amandine Jambert et Guilda Rostama, travaille spécifiquement sur la question, en essayant de trouver des solutions afin que les activités *blockchains* puissent rester dans le cadre de la loi « Informatique et libertés » et du règlement général sur la protection des données.

Leurs travaux se fondent sur l'étude de ce qui a été fait pour d'autres technologies ou dans d'autres pays, d'autres rapports, mais aussi des rencontres avec des acteurs. Il est à noter que la Commission a été saisie d'une trentaine de demandes de conseil émanant d'organisations envisageant l'utilisation de *blockchains*, le plus souvent de systèmes fermés.

Une fois qu'elles trouvent une position légalement et techniquement juste, elles proposent une explication puis des pistes de solution, qui pourront par exemple consister en une publication de prises de position sur le site de la CNIL.

Leurs rapports ont fait l'objet de différents débats particulièrement nourris. Le collège de la CNIL, qui se réunit tous les jeudis matin, a étudié le sujet à deux reprises. Sur les sujets techniques, le collège a besoin de travailler en deux temps pour comprendre la problématique puis prendre des décisions.

Particularité de l'analyse de la CNIL

La CNIL a un regard particulier avec une lecture très particulière qui se fait dans le cadre de la loi, c'est-à-dire une analyse légale. Cependant, lorsque la plénière l'estime nécessaire, elle peut appeler à un débat parlementaire. Cela dit, la CNIL travaille dans le respect des positions et des compétences de chacun.

Par ailleurs, puisque la loi est très récente et la *blockchain* très évolutive, la position peut difficilement être fixée.

Rappels sur la RGPD

La CNIL rappelle les définitions données par la loi et le règlement des termes données personnelles (identifiants ou potentiellement identifiants), traitement, responsable de traitement…

Elle rappelle aussi les cinq grands principes que sont :

- le principe de finalité ;

- le principe de proportionnalité ;

- le principe de conservation limitée ;

- le principe de sécurité ;

- le principe de confidentialité.

Ces principes forment une grille de lecture qui s'articule avec les droits des personnes :

- droit à l'information ;

- droit d'opposition ;

- droit d'effacement ;

- droit d'accès ;

- droit de rectification ;

- droit de portabilité, apport du RGPD qui constitue pour un responsable de traitement à l'exigence de communication, dans un format accessible, des données personnelles d'un utilisateur pour qu'il puisse les communiquer à son tour à un autre responsable de traitement.

Identifier le responsable de traitement

Pour la CNIL, la *blockchain* n'est pas un traitement en soi, mais une technologie. Toutes les personnes qui stockent ou déplacent des données ne sont en effet pas nécessairement des responsables de traitement. Le parallèle peut être fait avec un fournisseur d'espace serveur, **le responsable de traitement est celui qui a choisi d'entrer les données**.

En ce qui concerne Bitcoin, il est possible d'insérer des données personnelles avec la fonction *OP-Return*. Ainsi par exemple, un établissement d'enseignement supérieur parisien a décidé d'inscrire les hashs des diplômes qu'elle délivre sur la *blockchain*.

On peut distinguer trois types de personnes : des participants, des mineurs et des accédants, le responsable de traitement est le participant. En ce qui concerne les *smart contracts*, on peut estimer que celui qui le met en place est responsable de traitement.

En ce qui concerne, par exemple, un échange de bitcoin sans intermédiaire, il n'y a pas besoin d'un responsable car on se trouve hors du champ d'application du droit à la protection des données. La loi prévoit en effet une « exemption domestique » : lorsque le traitement s'applique entre deux personnes physiques en dehors de toute activité professionnelle, ce n'est pas un traitement au sens du RGPD.

Pour l'exemption de certains droits il faut une base légale, on pense habituellement au consentement mais il peut y en avoir d'autres.

Il est à noter que la CNIL travaille sur les deux types de *blockchains*, publiques ou privées, même si ce sont les premières qui posent le plus de difficultés.

Blockchain et droit des personnes

En ce qui concerne le **droit à l'oubli**, il existe quelques solutions techniques qui ne consistent pas exactement à « oublier la donnée » mais qui arriveraient à un effet similaire pour la personne car la donnée ne serait plus du tout accessible. Cependant, ce n'est pas tout à fait équivalent à un vrai droit à l'oubli. Ces solutions sont d'ordre informatique, la donnée peut être cachée, ou cryptographique, avec un chiffrement.

Cependant, la *blockchain*, en particulier publique, pourra difficilement être pleinement compatible avec le RGPD. La position pragmatique de la CNIL est de réfléchir à des solutions techniques permettant une minimisation des risques.

Certains acteurs ont intégré dans leurs *blockchains* des solutions pour leur conformité au RGPD avec une gestion du consentement. La communication publique sera axée sur ces différentes possibilités de répondre à l'exigence de responsabilisation des responsables de traitement.

Les *blockchains* sont souvent conçues dans l'idée qu'elles vont fonctionner *ad vitam aeternam*, alors qu'elles ne fonctionneront en pratique que tant que les mineurs seront actifs. Par ailleurs, d'un point de vue cryptographique, les fonctions utilisées aujourd'hui ne seront pas les mêmes que dans une vingtaine d'année.

Ainsi, au titre de cette responsabilité, il va être important de réfléchir dès leur conception à la mise à jour de ces fonctions. Si jamais un jour la fonction de hashage utilisée est cassée, un plan de gestion de crise est-il prévu ? Suivant le type de

blockchain, comment s'assurer que l'on ait suffisamment de mineurs de façon à ce qu'il n'y ait pas de coalition nuisible ?

Incompatibilités entre blockchain et RGPD

Par défaut, la *blockchain* n'apporte pas de confidentialité, mais de l'intégrité.

Le RGPD interdit les transferts de données hors Union européenne, à moins que les gestionnaires de données soient déclarés selon une certaine procédure. Dans le cadre d'une *blockchain* publique, où les mineurs sont répartis tout autour du globe et ne sont pas connus, cette exigence représente une véritable pierre d'achoppement.

Stratégie de la CNIL

À l'échelle européenne, très peu d'autres autorités en charge de la protection des droits sur les données personnelles se sont attaquées au sujet. On peut citer le cas de la Hongrie, qui n'a pas du tout la même approche en reconnaissant que les *blockchains* constituent un traitement en soi. Il faudrait établir des contacts plus poussés pour comprendre ce qui motive une telle analyse.

La stratégie de la CNIL c'est d'aider les entreprises à trouver des solutions de minimisation du risque pour les données afin de les aider à utiliser leurs technologies.

Il est difficile de répondre aujourd'hui à la question de savoir si l'on interdira l'utilisation de *blockchain* pour contradiction au RGPD. De toute manière, la réflexion de la CNIL est neutre technologiquement, de sorte qu'il ne peut y avoir une interdiction générale.

4. M. Georg Fuchsbauer, chercheur au département d'informatique de l'ENS

Différents modèles de consensus

En termes de consensus, les approches principales sont la *proof of work*, la *proof of stake* et d'autres alternatives, comme la *proof of space,* développée par Georg Fuchsbauer avec l'IST Austria et le MIT.

Le grand inconvénient conceptuel de la *proof of stake*, par rapport à la *proof of work*, c'est qu'il n'y a plus de distinction entre mineurs et détenteurs de pièces. Or dans une *blockchain* publique tout dépend du fait que ceux qui possèdent de l'argent soit intéressés par le processus de minage.

Puisque c'est un système ouvert, on ne peut pas concevoir un protocole qui va choisir des utilisateurs au hasard car il y aurait un risque d'attaque *Sybil*. Il faut donc se baser sur des ressources : dans la *proof of work* c'est la puissance de calcul tandis dans la *proof of space* c'est la taille d'espace disque. En effet, la mémoire est une vraie ressource qui a une valeur.

L'avantage de la *proof of space* c'est que chacun joue à armes égales en termes d'efficacité, la probabilité de « miner » un bloc est proportionnelle à la taille d'espace disque vide mise à disposition du réseau.

A l'inverse, dans la POW, il est possible de créer des calculateurs infiniment plus efficaces que la carte graphique d'un simple ordinateur, il y a donc une prime à ceux qui peuvent fabriquer à la chaîne leurs propres machines ultraspécialisées. Le fait que l'on puisse optimiser le calcul donne des avantages aux mineurs de grande taille.

Par ailleurs, la masse de machines à réseaux ASICS produite pour résoudre des fonctions de hashs ne peut avoir d'autre utilité, tandis que les disques durs pourront être réutilisés en cas de besoin pour d'autres usages.

La monnaie anonyme Zcash utilise « *eqh* » (*equihash* pour « *equalitarian computing* »), une fonction de hashage qui, en théorie, ne donne pas d'avantage disproportionné aux acteurs bénéficiant d'une importante puissance financière.

Il faut toutefois noter qu'en changeant les systèmes de hashage ou en utilisant de l'espace disque disponible, il est possible d'éviter la concentration, mais le problème de croissance exponentielle de la consommation énergétique subsiste.

Solutions techniques pour l'anonymat

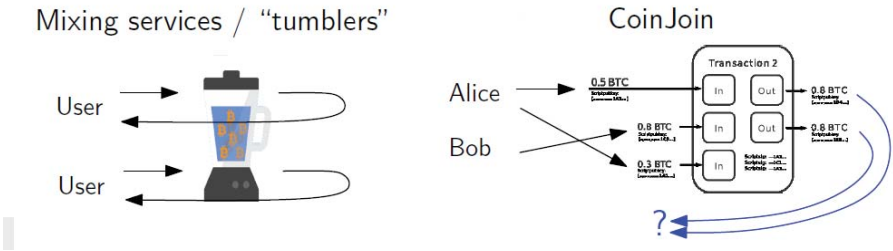
Bitcoin est pseudonyme, car toutes les transactions sont publiques et les adresses sont connues. « ***L'anonymat permet certes de protéger le droit à la vie privée, mais il est aussi utile pour des questions de fongibilité : en effet les mineurs pourraient décider de pénaliser un utilisateur en refusant de valider les transactions comprenant ses pièces*** ».

Un des premiers projets permettant d'anonymiser les transferts sur bitcoin fut le « mixage » (*mixing*), l'idée étant de mélanger les satoshis d'un utilisateur en les envoyant à une adresse qui elle-même se chargeait de les réorienter vers de nouvelles adresses, après plusieurs échanges « fictifs ». Le principal problème de cette solution est qu'elle suppose une confiance absolue dans le propriétaire de l'adresse de mixage pour qu'il ne s'accapare pas les bitcoins et qu'il ne révèle pas les émetteurs et destinataires des transactions.

Par ailleurs, certaines méthodes ont permis de remonter la trace d'utilisateurs ayant bénéficié de ce service, la sécurité du service dépendant des autres utilisateurs et du volume de transactions.

Une autre solution, *CoinJoin*, revient à mélanger les transactions de plusieurs utilisateurs, de sorte qu'on ne puisse plus savoir auquel appartenait tel ou tel satoshi. Elle a l'avantage d'éviter que quiconque ne puisse voler les satoshis, mais présente l'inconvénient de révéler aux autres participants les émetteurs et les destinataires des transactions.

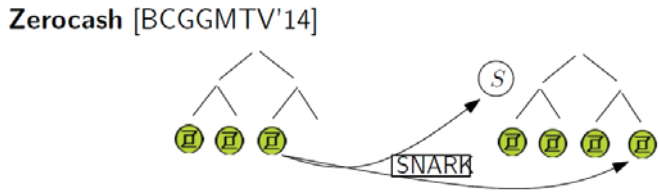
Enfin, sur Bitcoin, pour protéger le destinataire d'un paiement, il suffit que celui-ci créée plusieurs adresses et ne les utilise qu'une seule fois chacune. Cependant, cela n'est pas pratique dans tous les cas, par exemple pour une entreprise qui veut ne publier qu'une seule adresse pour tous ses potentiels clients.



La cryptomonnaie *Monero* utilise des « signatures d'anneau » (*ring signatures*) : lorsqu'un paiement est effectué, plusieurs pièces (*accounts*) sont inscrites, formant un « anneau » de clés, mais seule une sera effectivement utilisée. La signature camoufle laquelle a été précisément utilisée, on parle alors ici d'adresses furtives (*stealth addresses)*. Cette solution permet de ne publier qu'une seule adresse et les émetteurs du paiement restent intraçables.

Il est aussi possible de cacher les montants de la transaction grâce à la cryptographie, tout en laissant savoir qu'elle a eu lieu et que l'entrée et la sortie d'un bloc sont égales en termes de transactions, donc qu'il n'y a pas eu de fraude.

Fonctionnant avec ce système de *zero knowledge proof*, Zcash est aujourd'hui la monnaie la plus anonyme. Elle utilise des zk-SNARKs (*zero knowledge succinct non-interactive argument of knowledge*) qui sont des preuves *zero knowledge*, c'est-à-dire sans divulgation de connaissance, qui ne nécessitent pas d'interaction préalable entre les utilisateurs (*non-interactive*).



Zcash présente toutefois deux limites importantes à son déploiement. D'une part, ces processus d'anonymisation rendent le système environ 1 000 fois plus lent qu'une *blockchain* publique classique. D'autre part, il est nécessaire qu'une personne inscrive des paramètres d'origines, qui doivent être tenus secret, celle-ci peut à ce moment-là potentiellement produire de la monnaie de contrefaçon sans que quiconque ne puisse s'en apercevoir.

Cela dit, même si les paramètres ont été malicieusement établis, les SNARKs sont résistants aux subversions, ce qui signifie que l'anonymat subsiste en tout état de cause.

Alternatives à la proof of work et aux blockchains

Georg Fuchsbauer est sceptique quant à l'utilisation des graphes acycliques dirigés (DAG), dont le fonctionnement est loin d'être prouvé. En ce qui concerne IOTA en particulier, il fait remarquer que cette solution utilise des standards non habituels de cryptographie.

Malgré son travail sur la *proof of space,* il reconnaît que la *proof of work* reste un protocole beaucoup plus simple que toutes les autres méthodes de consensus.

REUNION DE L'OFFICE DU 12 AVRIL 2018 : EXAMEN D'UNE NOTE COURTE SUR LES CHAINES DE BLOCS (*BLOCKCHAINS*)

M. Claude de Ganay, député. - Je rappelle, à titre liminaire, que notre travail répond à une demande de la mission d'information commune créée à l'Assemblée nationale sur « les usages des *blockchains* et autres technologies de certification de registres », présidée par notre collègue Julien Aubert. Cette note courte sera suivie d'une note plus développée d'ici la fin du mois de mai.

Nous nous sommes répartis cette présentation de la manière suivante : je reviendrai sur les origines des *blockchains* ou chaînes de blocs, Ronan Le Gleut décrira leur fonctionnement de manière détaillée et Valéria Faure-Muntian abordera, pour conclure, la question de certains enjeux technologiques, à savoir le défi de la capacité des *blockchains* à monter en charge, les *smart contracts* ou contrats intelligents, la distinction entre *blockchains* publiques et *blockchains* privées et, enfin, la question de leur consommation énergétique.

Pour comprendre ces technologies, nous proposons une définition : les chaînes de blocs ou *blockchains* sont des technologies de stockage et de transmission d'informations permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers. Pour comprendre le fonctionnement de ces registres informatiques, utilisés dans des réseaux décentralisés pair à pair (*peer to peer*), et qui forment les technologies sous-jacentes aux cryptomonnaies, il est nécessaire de revenir à leurs origines. Les cryptomonnaies s'inscrivent dans le sillage du mouvement pour le logiciel libre et de la communauté « cypherpunk ». Le mot-valise « cypherpunk » est formé à partir de l'anglais *cipher* ou chiffrement et « cyberpunk », lui-même issu des mots cybernétique et punk et renvoyant à des œuvres de fiction dystopiques basées sur les technologies.

Ces deux communautés, qui peuvent se recouper, étaient depuis longtemps désireuses d'utiliser les technologies de chiffrement pour créer un outil de paiement électronique et garantir des transactions anonymes. Les premières tentatives ont été des échecs. C'était le cas de e-cash et digicash en 1983 et 1990 avec David Chaum, puis en 1998 de b-money avec Wei Dai et, surtout, de bitgold avec Nick Szabo. L'invention de hashcash par Adam Back en 1997 avait pourtant marqué un progrès avec l'idée de valider les transactions par la résolution de fonctions de hachage cryptographiques, appelées « preuves de travail ». L'objectif de ces technologies est de rendre inutile l'existence d'un « tiers de confiance », en recourant à un système de confiance distribuée permettant de constituer une sorte de « grand livre comptable » infalsifiable.

L'obstacle à lever résidait dans le problème de la double dépense, c'est-à-dire le risque qu'une même somme soit dépensée deux fois et, plus généralement, dans celui de la tolérance aux pannes, qu'elles soient accidentelles ou malveillantes : ce qu'on appelle en informatique le problème des généraux byzantins[1].

La réponse à ces difficultés est apportée en 2008 dans un article de Satoshi Nakamoto, pseudonyme du collectif des fondateurs du bitcoin et de la première *blockchain*. Cet article décrit le fonctionnement d'un protocole infalsifiable utilisant un réseau pair à pair - la *blockchain* - comme couche technologique d'une nouvelle cryptomonnaie – le bitcoin.

M. Ronan Le Gleut, **sénateur**. – Le bitcoin repose sur un protocole sous-jacent appelé *blockchain* : il est le premier cas d'usage de cette technologie. On parle de chaînes de blocs ou *blockchains* car les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs « horodatés » : ces transactions reposent sur une cryptographie asymétrique, avec une paire de clés, l'une privée et l'autre publique.

Une fois le bloc validé grâce à une « méthode de consensus », appelée « preuve de travail » (*proof of work*) dans le cas du bitcoin, la transaction devient visible pour l'ensemble des détenteurs du registre, qui vont alors l'ajouter à leur chaîne de blocs. Je précise que chaque bloc possède un identifiant chiffré, appelé « hash », car l'algorithme de chiffrement utilisé est appelé « fonction de hachage ». Dans le cas du bitcoin, cet algorithme s'appelle SHA-256, pour *Secure Hash Algorithm-256*, ainsi nommé car il produit des hashs d'une taille de 256 bits.

La preuve de travail suppose la réussite à une épreuve cryptographique dénommée « minage » : elle consiste en la résolution par certains utilisateurs du réseau appelés mineurs, de problèmes utilisant les fonctions de hachage. Il faut noter que cette opération, très coûteuse en puissance de calcul informatique, est motivée par l'obtention d'une récompense en bitcoins par le mineur gagnant. La rémunération des mineurs est complétée par des frais prélevés sur les transactions qu'ils intègrent à chaque nouveau bloc. L'organisation des mineurs en groupements ou « *pools* » induit le risque qu'une majorité organisée oriente la validation des blocs.

La confiance des utilisateurs dans le système étant un objectif partagé par les mineurs, celle-ci est censée suffire à garantir le respect des règles, dans une logique de « main invisible » protégeant les intérêts privés. Quatre *pools* dont trois chinois assurent aujourd'hui plus de 60 % de la puissance de calcul nécessaire à la *blockchain* du bitcoin et pourraient utiliser cette position dominante contre l'intérêt des autres utilisateurs.

D'autres méthodes de consensus que la « preuve de travail » existent mais elles sont souvent plus centralisées, la principale alternative, qui présente aujourd'hui un risque plus grand d'utilisation malveillante, est la « preuve d'enjeu », appelée aussi « preuve de participation » *(proof of stake),* basée sur la possession de cryptomonnaies mises en séquestre.

Ma dernière remarque porte sur la manière de modifier les règles régissant une *blockchain*, on parle alors d'embranchement ou *fork*. Toute personne peut proposer des

---

[1] *En informatique, le problème des généraux byzantins est une métaphore qui traite de la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs. La question est donc de savoir comment, et dans quelle mesure, il est possible de prendre en compte une information dont la source ou le canal de transmission est suspect. La solution implique l'établissement d'un algorithme adapté. Ce problème a été traité en profondeur pour la première fois dans l'article « The Byzantine Generals Problem », publié en 1982.*

modifications mais elles émanent le plus souvent de quelques développeurs : un noyau d'une quarantaine dans le cas du bitcoin. On distingue deux types d'évolutions : les *soft forks*, lorsque les blocs produits sous la nouvelle version peuvent être ajoutés par des nœuds fonctionnant encore sous l'ancienne version, et les *hard forks*, lorsqu'une telle rétrocompatibilité est impossible. Lorsqu'ils ne sont pas adoptés à l'unanimité, ces *hard forks* peuvent donner naissance à des *blockchain*s alternatives et indépendantes de la version originelle. En 2017, bitcoin cash et bitcoin gold sont ainsi nés de *hard forks* du bitcoin d'origine.

Mme Valéria Faure-Muntian, députée. - J'en arrive à certains enjeux technologiques des *blockchains*, à savoir le défi de la capacité des *blockchains* à monter en charge, les *smart contracts*, la distinction entre *blockchains* publiques et *blockchains* privées et la question de leur consommation énergétique.

La capacité à faire face à une augmentation du nombre de transactions, appelée « scalabilité », constitue l'un des principaux défis pour les *blockchain*s, à commencer par celle du bitcoin. Ce défi a conduit à accélérer la naissance d'autres cryptomonnaies, dites alternatives (« altcoins »), plus de 1 500 à ce jour. Il a également mené à des innovations encore souvent peu matures d'un point de vue technologique. Bien que le rôle de la *blockchain* en tant que technologie sous-jacente des nombreuses cryptomonnaies soit aujourd'hui dominant, ses protocoles se déclinent dans de nombreux secteurs et pourront donner naissance à des applications nouvelles variées, dépassant le cadre strict de la finance : par exemple, des services d'attestation et de certification pouvant concerner l'état civil, le cadastre, des contrats de type notarié ou, encore, des mécanismes de protection de la propriété intellectuelle. Mais peu d'applications conjuguent, à ce jour, pertinence de l'usage et maturité technologique suffisante.

On peut relever que la *blockchain* Ethereum offre une infrastructure adaptée à des outils tels que les *smart contracts*, codes informatiques qui ne sont pas des contrats au sens juridique et qui peuvent s'exécuter après avoir été écrits dans une *blockchain*. Par rapport à des programmes classiques, les *smart contracts* présentent l'avantage de bénéficier des caractéristiques particulières de la *blockchain*. Ainsi, leur exécution est irrémédiable et leur code est vérifiable librement par les nœuds du réseau. Ils permettent aussi de placer des fonds sous séquestre de manière vérifiable. J'indique que l'exécution de la plupart des *smart contracts* reste conditionnée par l'apport et l'export d'informations : que ce soit pour relever une température, livrer un colis, prouver la réalisation d'un travail, ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'oracle dans l'écosystème Ethereum, doit faire le lien entre la *blockchain* et le reste du monde, ce qui s'apparente au retour d'un « tiers de confiance », alors que la *blockchain* devait permettre de s'en passer.

La distinction entre *blockchains* publiques et *blockchains* privées ne repose pas sur une distinction entre *blockchains* de personnes publiques et *blockchains* de personnes privées mais sur le caractère ouvert (*permissionless*) ou fermé (*permissioned*) de la *blockchain*. Un débat existe pour qualifier les *blockchain*s privées de « vraies » ou de « fausses » *blockchain*s, sachant que créer un produit recourant à ces technologies est aussi un enjeu de marketing : le recours aux *blockchains* pour certaines applications ne semble pas toujours justifié, les fonctionnalités offertes par les bases de données partagées et sécurisées existantes apparaissant, en effet, suffisantes à leur réalisation, d'autant plus que des technologies alternatives de registres distribués sont en développement. Le succès des levées de fond spécifiques à l'écosystème des cryptomonnaies, appelées ICO pour *Initial Coin Offering*, interroge également : sont-elles vraiment rationnelles ?

Nous estimons qu'un regard distancié paraît nécessaire, en raison des effets de mode propres aux écosystèmes entrepreneuriaux qui ne s'accompagnent pas toujours d'innovations aussi majeures que celles annoncées.

Je souhaite conclure avec les enjeux énergétiques et environnementaux des *blockchain*s, surtout pour celles fondées sur la preuve de travail : les besoins en électricité des *blockchains* sont considérables. Leur estimation fait l'objet de débats mais la consommation pour le seul bitcoin est d'au moins 24 TWh/an, ce qui représente la production totale annuelle de 3 réacteurs nucléaires de 8 TWh. Depuis la création du bitcoin, ces besoins ne font qu'augmenter de manière quasi-exponentielle. L'impact en termes d'émissions de gaz à effet de serre est d'autant plus important que les groupements de mineurs sont surtout établis en Chine, pays qui présente, pour sa production électrique, l'intensité carbone la plus élevée au monde. J'espère que cette note contribuera à ce que la recherche relève ce défi de la consommation énergétique des *blockchains*.

M. Gérard Longuet, sénateur, président de l'Office. – Je remercie nos trois collègues qui ont fait un travail impressionnant et qui ont un avantage sur nous, celui de maîtriser ce sujet, qui est à la fois passionnant et vertigineux. Il est difficile de comprendre parfaitement les contraintes et les perspectives des *blockchains*. L'une des premières pistes consiste à supprimer le tiers de confiance, ce qui est une idée relativement séduisante, de nature à remettre en cause les organisations administratives ou privées tout en apportant une réponse convaincante. La deuxième piste intéressante est celle de la contestation du monopole de certaines fonctions exercées par les pouvoirs publics, à commencer par la création de monnaie. Il s'agirait d'échapper au système centralisé des monnaies nationales, comme le dollar, ou internationales, comme l'euro. Est-ce que vous avez réfléchi sur ces deux aspects ? Le premier porte sur la question du tiers de confiance et, donc, de l'administration, y compris l'administration fiscale, ou de quasi-administrations comme les notaires pour la gestion des actifs immobiliers. Le deuxième revient à se demander si le regard un peu goguenard sur ce type de monnaie des autorités monétaires centrales, y compris de la Banque de France - je l'ai vu à la commission des finances du Sénat - est justifié ou s'il faudrait mieux se méfier de ce système, qui peut déborder rapidement ces autorités, dans une société où le numérique permet à la fois de ficher tout le monde et de libérer chacun des systèmes de contrôle centralisés.

M. Ronan Le Gleut, sénateur. – Ces questions ont plus que du sens, elles touchent véritablement le fondement même des problématiques soulevées par les technologies *blockchains*. Premièrement, il me semble important de dire qu'il s'agit d'un sujet de la plus grande importance. Quelques chiffres pour en témoigner : la valorisation actuelle de l'ensemble des crypto-actifs est de 271 milliards de dollars, 123 milliards de dollars pour le bitcoin seul, pour l'ether, qui est la deuxième cryptomonnaie, 39 milliards de dollars et pour le ripple, qui est la troisième, 19 milliards de dollars. Vous avez employé le mot vertigineux, nous y sommes. Il faut mesurer à quel point le sujet est sérieux.

Ensuite, la question du tiers de confiance est effectivement essentielle parce qu'on a affaire à quelque chose de révolutionnaire. Ce en quoi croient les libéraux depuis toujours, c'est-à-dire l'idée minoritaire selon laquelle il peut y avoir une forme d'autorégulation et que la « main invisible » d'Adam Smith existe, semble fonctionner depuis dix ans avec la *blockchain* du bitcoin. Son invention remonte à un papier publié sur internet en 2008 et sa mise en œuvre à 2009. Aujourd'hui, en 2018, il y a eu certes des tentatives de déstabilisation, mais ce système fonctionne et s'autorégule depuis dix ans. On a donc affaire à quelque chose de phénoménal, qui prend des dimensions économiques considérables et qui fonctionne sans tiers de confiance.

M. Gérard Longuet, sénateur, président de l'Office. – Dans un monde où des systèmes informatiques de très grande puissance, y compris les systèmes de services de renseignement théoriquement fiables comme ceux de la CIA ou de la DGSE, sont piratés par des intervenants extérieurs, on a peine à croire qu'une chaîne de blocs suffise à échapper à cela et que le contrat que l'on va y écrire ne va pas être, à un moment ou un autre, modifié ou dénaturé par une entité extérieure.

M. Ronan Le Gleut, sénateur. – Je précise qu'il y a, tous les jours, des tentatives pour faire exploser ce modèle de chaînes de bloc et qu'il y a aussi, tous les jours, des développeurs qui adaptent le système. En fait, deux sujets doivent être distingués : la dimension technique et la dimension philosophique. Quand on interroge les acteurs, il y a une dimension philosophique évidente à leur action : ils y « croient », et quand on interroge un certain nombre de gens qui pourraient être, aujourd'hui, potentiellement riches en vendant leurs bitcoins et qui ne veulent pas le faire, on constate qu'ils défendent l'idée qu'on peut avoir un système autorégulé et qu'ils ne veulent pas fragiliser un projet auquel ils croient. Ce système repose sur une part de conviction : le soutien à cette technologie est lié à l'idée que le monde peut fonctionner sans tiers de confiance et, qu'à la place, il peut y avoir un système de confiance mutuelle. Cette dimension philosophique est absolument essentielle dans le succès et la compréhension de la *blockchain*. Sur la dimension technique, j'observe que la *blockchain* est attaquée tous les jours et qu'en faire un bilan dix ans après permet de se rendre compte que ce système a tenu. Il n'est évidemment pas inattaquable, car aucun système ne l'est, mais il se trouve qu'il a tenu jusqu'à aujourd'hui. Il faut aussi savoir qu'il évolue plusieurs fois par an : les développeurs se mettent d'accord sur des évolutions qui font progresser le modèle de départ, les *soft forks* dont j'ai parlé tout à l'heure.

M. Gérard Longuet, sénateur, président de l'Office. – C'est une communauté ou une organisation ?

M. Ronan Le Gleut, sénateur. – On touche là un point fondamental : ce n'est pas une organisation mais une communauté de gens qui y croient et qui veulent que ça fonctionne. Ils travaillent donc, souvent d'ailleurs gratuitement, pour apporter des modifications au code informatique de départ qui, donc, s'améliore progressivement et a fait la démonstration de sa solidité.

M. Gérard Longuet, sénateur, président de l'Office. – C'est une communauté autogérée ?

M. Ronan Le Gleut, sénateur. – Absolument, cette communauté est autogérée en permanence autour de forums des développeurs, dont un a été mis en place par le créateur du bitcoin lui-même. Ce créateur mystérieux, dont on ne connaît pas l'identité, est en fait probablement un groupe de cinq ou six experts qui ont travaillé ensemble, unis par une philosophie commune. L'idée de forum correspond à la possibilité, pour les développeurs, de commenter en permanence ce qui se passe sur la *blockchain*. Le forum créé par le créateur du bitcoin est toujours utilisé aujourd'hui.

Mme Valéria Faure-Muntian, députée. - Le système est organisé de manière à être le plus démocratique possible : tout le monde peut donc intervenir sur la *blockchain*. C'est le consensus, l'accord de l'ensemble des acteurs, qui fait qu'elle pourra être modifiée ou pas. Une modification peut donc être rejetée si tout le monde n'est pas d'accord. En ce qui concerne la question de savoir si la chaîne est attaquable, elle l'est certes, comme tout système informatique, mais son organisation démocratique fait qu'il y a de nombreuses protections. Si jamais plusieurs chaînes coexistent, il existe ainsi un consensus pour que seule la chaîne la plus longue soit conservée. Cette validation successive par de nombreux intervenants fait que la chaîne est considérée comme solide. Vous avez utilisé le terme de

« tiers de confiance », or, sur la *blockchain*, tout participant peut valider un bloc en devenant mineur ou détenir une sauvegarde chez lui sur son ordinateur, il n'y a donc en effet pas de tiers de confiance, tout est décentralisé et l'on parle de système « pair à pair », c'est-à-dire fonctionnant de particulier à particulier. Tout le monde peut faire une intervention, passer une commande ou réaliser une transaction.

M. Gérard Longuet, sénateur, président de l'Office. – Peut-on y faire une transaction commerciale ?

Mme Valéria Faure-Muntian, députée. – Oui.

M. Cédric Villani, député, premier vice-président de l'Office. - Je souhaite d'abord féliciter chaleureusement nos collègues qui se sont investis dans cette mission, dont je rappelle qu'elle s'inscrit en soutien à la mission d'information commune aux trois commissions des affaires économiques, des finances et des lois de l'Assemblée nationale sur « les usages des *blockchains* et autres technologies de certification de registres », présidée par notre collègue Julien Aubert avec deux co-rapporteurs, Laure de La Raudière et Jean-Michel Mis.

Nous nous étions entendus avec eux pour leur apporter un soutien technique avec un travail qui pourrait les aider à dégager les enjeux de cette technologie. Je pense que cette note courte est une première étape, qui apporte un début de réponse et qui sera tout à fait utile. Je suis frappé par la qualité du travail qui a été accompli en un temps record.

Nous voyons précisément ici comment il est possible de répondre à une demande sur un sujet qui est en évolution rapide et qui relève des sciences et technologies mais, aussi, comme vos réponses l'ont bien souligné, de choix politiques, idéologiques et philosophiques qui sous-tendent la démarche d'usage des *blockchains*. Celles-ci portent un vrai changement, avec la possibilité de réaliser des transactions dont la fiabilité est garantie, non pas par une organisation ou par une personne, mais par une communauté. Si l'on voulait pirater le système, il faudrait agir sur l'ensemble de la communauté, ce qui lui donne une stabilité très forte. Bien sûr, ces systèmes peuvent être soumis à des mouvements de foule, des changements d'idéologie ou bien à des actions politiques agissant sur une communauté de grande dimension. Ce que Ronan Le Gleut a pu dire sur le rôle de la Chine était ainsi particulièrement intéressant : je n'avais pas conscience du point auquel ce système est exposé à une potentielle fragilité liée à l'influence chinoise.

Il est aussi intéressant que notre collègue ait évoqué le rôle des conceptions libertariennes, selon lesquelles il faut donner le rôle le plus réduit possible aux autorités étatiques et le plus grand à une sorte de « main invisible », qui sous-tendrait l'ensemble. Ce côté « absolu » permis par la technologie, et qui est recherché par les participants, peut être une fragilité pour l'évolution de la technologie elle-même. En effet, on sent qu'elle pourrait être utilisée avec des modes « mixtes » de gouvernance et qu'il existe un débat sur la question de systèmes privés ou publics, la question étant de savoir si un système fermé doit être qualifié de *blockchain*. Ces controverses montrent bien l'aspect idéologique sous-jacent qui, à titre personnel, me pose beaucoup de questions, notamment l'idée de faire totalement confiance à cette technologie qui peut sembler assez effrayante.

Je m'interroge aussi sur l'idée d'oublier, ou de mettre au second plan, le défi environnemental qui paraît considérable, du moins si l'on utilise la technologie dans son mode le plus ouvert et le plus absolu, avec la preuve de travail. À titre personnel, c'est ce problème qui me pose le plus de questions.

Je suis également frappé par le fait que l'on dise que le système s'autorégule alors que l'on observe tout de même une volatilité considérable par rapport à une monnaie classique. Lorsque l'on parle d'une capitalisation de 130 milliards de dollars du bitcoin, on peut

se dire que c'est soit une opportunité phénoménale, soit une des plus grandes bulles jamais vues et qu'elle explosera en créant un chaos dont on ne pourra tenir personne pour responsable.

Mme Catherine Procaccia, sénatrice, vice-présidente de l'Office. –Merci beaucoup pour la présentation et la note même si j'avoue que j'ai encore un peu de mal à tout comprendre. Ma question est la suivante : vous avez présenté la sécurité de ce système mais, s'il est si sûr que cela, pourquoi n'est-il pas appliqué dans d'autres secteurs ? On parle beaucoup ici des cryptomonnaies, mais elles sont en marge de tous les systèmes officiels et je présume qu'elles permettent aussi la fraude fiscale… Autrement dit, cette note parle beaucoup d'avenir mais j'ai du mal à voir cet avenir pour nous les usagers, pour les États, pour les gouvernements, etc. Si l'on se sert de cette technologie d'abord pour sécuriser les monnaies, peut-on le faire ensuite pour d'autres transactions qui, pour l'instant, ne sont pas sécurisées, qu'elles soient monétaires ou non ?

M. Claude de Ganay, député. – Dans cette note, nous nous sommes limités à la définition de la technologie et à son fonctionnement, ce qui répond à une demande de la mission présidée par Julien Aubert qui, elle, travaille davantage sur les usages. Notre travail répond pleinement à la mission de l'Office : apporter des éclairages en amont des travaux des autres parlementaires. Nous avons prévu de compléter cette note et de produire un document plus complet avant la fin du mois de mai prochain.

M. Ronan Le Gleut, sénateur. – Vous avez posé beaucoup de questions. Un point extrêmement important est le sujet de la volatilité et, donc, de la possibilité que cette monnaie puisse se substituer à d'autres. Je vais beaucoup vous surprendre mais la volatité du bitcoin est en baisse. Beaucoup d'articles ont commenté le cours du bitcoin, notamment lorsqu'il a atteint près de 20 000 dollars au mois de décembre 2017, alors qu'il est revenu autour de 7 000 ou 8 000 dollars aujourd'hui. Mais lors des premières années qui ont suivi la création du bitcoin, en 2009 et 2010, la volatilité était bien supérieure, le cours du bitcoin était, par exemple, un jour autour d'un dollar et pouvait passer à 32 dollars le lendemain, puis redescendre : on perdait alors 32 fois sa mise, ce qui est à comparer au fait de passer aujourd'hui « seulement » de 20 000 à 8 000 dollars. Si cette volatilité baisse depuis le lancement du bitcoin en 2009, c'est pour une raison simple : plus les volumes sont importants, moins on peut jouer sur les cours. Par ailleurs, il faut tout de même rappeler que « jouer les monnaies » n'a pas été inventé avec les cryptomonnaies.

M. Gérard Longuet, sénateur, président de l'Office. – Et pas non plus par George Soros !

M. Ronan Le Gleut, sénateur. – En ce qui concerne la crainte d'une bulle, je pense qu'il faut s'inscrire dans le temps long : en l'état actuel des choses, il ne me semble pas que l'on puisse utiliser ce terme, seul l'avenir nous le dira.

Sur le défi environnemental, je suis en revanche d'accord, on a affaire à un vrai problème. Aujourd'hui, on est probablement autour de 50 TWh pour la consommation du seul bitcoin. Ce n'est pas tenable, surtout si le cours du bitcoin monte. Car il faut bien comprendre que cette consommation est liée à une compétition entre mineurs, organisés en « *pools* » d'ordinateurs, qui se rémunèrent en obtenant 12,5 bitcoins lorsqu'ils réussissent une épreuve de calcul. Il faut d'ailleurs noter que la France, et l'Europe en général, sont en dehors de cette compétition mondiale. Or quand on voit qu'un pays comme la Géorgie est capable d'installer sur son territoire une grande partie des infrastructures de Bitfury, un pool de mineurs très important, on doit s'interroger.

M. Gérard Longuet, sénateur, président de l'Office. – Je crois que l'informatique est un langage nouveau qui gomme les héritages culturels. Il est beaucoup plus facile, pour une nouvelle génération, de s'emparer de ces nouveautés que d'adapter les générations anciennes. Autrement dit, quand on n'a jamais fait de banque, il vaut peut-être mieux s'engager dans le bitcoin que de rejoindre une banque classique.

M. Ronan Le Gleut, sénateur. – La question environnementale est sérieuse et constitue un véritable problème. Le fait que le bitcoin ait une valorisation élevée va entraîner des investissements encore plus importants dans la compétition entre mineurs, et pourrait avoir ensuite une répercussion sur les cours mondiaux de l'électricité. On est là face à un véritable défi, dont les développeurs ont pris conscience en cherchant des techniques alternatives, comme celle du ripple par exemple. Mais le bitcoin ne répond pas à ce défi pour le moment.

Une autre de vos questions porte sur l'utilisation de la *blockchain* dans d'autres domaines que celui des cryptomonnaies. Le texte fondateur de Satoshi Nakamoto montre que la *blockchain* a été inventée dans le but de créer le bitcoin. À l'origine, la *blockchain* est au service du bitcoin et on n'anticipait pas vraiment d'autres utilisations possibles de la technologie. Aujourd'hui, beaucoup essaient d'utiliser cette invention majeure dans d'autres secteurs, mais on en est plutôt aux balbutiements. Un certain nombre de personnes travaillent sur ces sujets, mais je pense que les développements ne sont pas encore mûrs et relèvent plutôt de la prospective.

Sur la sûreté de la *blockchain* en tant que réseau, il n'y a aucune naïveté de notre part : aucun système n'est inviolable, nous en avons bien conscience, mais ce protocole a prouvé sa solidité pendant dix ans. J'observe d'ailleurs que d'autres systèmes peuvent s'effondrer, y compris un système étatique.

Mme Annie Delmont-Koropoulis, sénatrice. – Ronan Le Gleut a répondu à mes interrogations concernant le défi environnemental. Effectivement, ces technologies, au développement exponentiel, vont devenir un gouffre énergétique et les émissions de CO_2 vont être considérables.

Comme Catherine Proccacia, je me pose la question des autres utilisations possibles. Dans le domaine de la recherche médicale et des laboratoires pharmaceutiques, des transactions sécurisées et certifiées pourraient être intéressantes.

M. Cédric Villani, député, premier vice-président de l'Office. - Merci pour la suite de cette discussion. Je pensais aussi, en regardant votre note, à quel point il y a lieu d'être fiers de la liste d'experts que vous avez réussi à mobiliser et à interroger en un temps aussi réduit, surtout d'un aussi haut niveau.

M. Claude de Ganay, député. – Et pour beaucoup d'entre eux, il n'y a pas de redondance avec les experts auditionnés par la mission de Julien Aubert, ce qui est intéressant justement.

M. Cédric Villani, député, premier vice-président de l'Office. - Je suis parfaitement d'accord. Deux commentaires me viennent.

D'une part, sur la question que pose Catherine Procaccia de savoir pourquoi la technologie se développe pour l'instant surtout dans le domaine de la finance, à travers les cryptomonnaies : je crois que la finance est souvent un secteur qui expérimente beaucoup en matière de technologie, avec la capacité de lever des fonds beaucoup plus facilement que dans bien d'autres secteurs. C'est d'ailleurs la raison majeure pour laquelle nous n'avons pas intégré les banques et les assurances dans les secteurs prioritaires pour l'action de l'État dans mon rapport sur l'intelligence artificielle. Cela fait un moment que la finance se « débrouille » toute

seule et expérimente déjà, par exemple, l'intelligence artificielle. Dès qu'il y a une innovation, elle l'utilise et s'en empare en expérimentant. Je vous rappelle que c'est peut-être le secteur financier qui a porté le plus tôt les questions de numérisation et de révolution numérique en termes d'emplois. Les *traders* à l'ancienne se sont faits balayés par les *traders* algorithmiques bien avant que ce genre de problématique n'apparaisse dans d'autres secteurs. C'est donc peut-être pour cette raison que les systèmes financiers se sont lancés dans l'expérimentation des technologies *blockchain*.

D'autre part, je relève que les pères fondateurs et la communauté d'origine insistaient sur un mode de fonctionnement complètement dépourvu de figure d'autorité. Or on peut imaginer que, dans bien d'autres cas d'usages, il ne s'agira pas de systèmes sans autorité mais que certaines entités auront des droits particuliers et des prérogatives. Je pense, par exemple, à des applications dans des secteurs tels que le notariat, où l'autorité notariale voudra se réserver le droit de pouvoir faire telle ou telle modification puisqu'elle est responsable en cas de contestation. On n'est donc plus exactement dans l'idéal auquel aspiraient les pères fondateurs des *blockchains*.

M. Gérard Longuet, sénateur, président de l'Office. – Peut également être anticipé un choc à venir avec les systèmes existants, qui voudraient soit bloquer ces technologies soit se les approprier. Je remercie chaleureusement nos collègues députés et sénateur pour leur travail, sachant qu'ils vont continuer à travailler, en assurant une liaison avec la mission présidée par Julien Aubert. À nous, en tant que membres de l'Office parlementaire, de valoriser ce travail et de montrer la sagesse, la pertinence, la profondeur, l'acuité, la rapidité et la réactivité des parlementaires.

M. Cédric Villani, député, premier vice-président de l'Office. –Qu'ils reçoivent aussi tous mes encouragements en vue du rapport plus développé qu'ils vont produire d'ici environ deux mois.

REUNION DE L'OFFICE DU 14 JUIN 2018 : ADOPTION DU RAPPORT

M. Gérard Longuet, sénateur, président de l'Office. – Nous examinons le rapport sur les enjeux technologiques des *blockchains* de nos trois collègues, Valéria Faure-Muntian, Claude de Ganay et Ronan Le Gleut.

M. Claude de Ganay, député, corapporteur. – Le rapport que nous présentons ce matin fait suite à la note courte que nous avions présentée devant l'Office le 12 avril dernier. Nous ne reviendrons pas sur les éléments que nous avions alors exposés devant vous et aborderons plutôt les points approfondis à l'occasion de ce rapport. Je reviendrai sur les avantages et les inconvénients des différentes méthodes de consensus ainsi que sur les caractéristiques des *blockchains* propres à chaque cryptomonnaie. Ronan Le Gleut décrira les différentes applications possibles de ces technologies, les enjeux en matière de sécurité et les qualités et défauts des ICO (*Initial Coin Offerings*). Valéria Faure-Muntian abordera plusieurs grands enjeux des *blockchains*, à savoir la question de leur consommation énergétique, les problématiques juridiques ainsi que la question de leur diffusion à la lumière du principe de souveraineté, plaidant ainsi pour des *blockchains* européennes qui, sans être souveraines, respectent nos valeurs politiques, philosophiques et morales.

Je vous rappelle tout d'abord ce que sont les chaînes de blocs ou *blockchains* : il s'agit de technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers.

Les procédures par lesquelles les blocs sont validés sont dénommées méthodes de consensus. La plus ancienne et principale cryptomonnaie, le bitcoin, a recours à une compétition cryptographique appelée « preuve de travail » ou *proof of work* (POW), qui pose notamment un problème de consommation électrique ; c'est pourquoi des alternatives sont développées pour chercher à la remplacer. Cependant, ces autres méthodes présentent un risque de centralisation et leur sécurité est souvent moins certaine, avec un plus grand risque d'utilisation malveillante.

La principale alternative à la preuve de travail est appelée « preuve d'enjeu » ou *proof of stake* (POS), mais son déploiement reste lent. Son principe consiste à attribuer la validation de chaque bloc de manière aléatoire à un utilisateur, selon une probabilité qui n'est pas liée à une capacité de calcul spécialisée, comme c'est le cas pour la preuve de travail. La POS recouvre en réalité deux preuves distinctes : la preuve de participation, qui consiste à attribuer les blocs en fonction de la quantité de cryptomonnaies possédée par un nœud, tandis que la preuve d'enjeu, à proprement parler, va plus loin en exigeant de mettre en gage ces monnaies, qui seront détruites en cas de fraude. Des dérivés de la preuve d'enjeu existent : on peut citer la « preuve de possession » (*proof of hold*), fondée sur la durée de possession, la « preuve d'utilisation » (*proof of use*), en fonction du volume de transactions, la « preuve d'importance » (*proof of importance*), reposant sur la « réputation », la « preuve de capacité »

(*proof of space*), qui consiste à mettre en gage de l'espace disque disponible, ou encore la « preuve de destruction » (*proof of burn*), qui revient à détruire des cryptomonnaies pour obtenir la confiance du réseau.

On peut donc, pour simplifier, distinguer une méthode fiable et sécurisée mais lente et coûteuse en énergie, la preuve de travail, et une seconde méthode, plus économe tant en énergie qu'en matériel spécialisé mais à la sécurité encore contestée, la preuve d'enjeu. Celle-ci est difficile à mettre en place et n'a toujours pas été adoptée par Ethereum, dont le passage à la preuve d'enjeu est prévu depuis l'origine mais a été repoussé à plusieurs reprises depuis deux ans. En termes de pourcentage de la capitalisation de l'ensemble des monnaies cryptographiques, les monnaies reposant sur la preuve de travail sont passées de 99 % en 2013 à 80 % en juin 2018. Certains acteurs estiment qu'une *blockchain* ouverte sans preuve de travail ne peut fonctionner.

Toutes les *blockchains* des 1 600 cryptomonnaies existantes sont plus ou moins des avatars de celle du bitcoin. Je ne reviens pas sur le détail de ces 1 600 systèmes, je relève surtout l'ouverture de nouvelles perspectives grâce au protocole Ethereum évoqué à l'instant, appuyé sur la monnaie ether. Celui-ci facilite l'automatisation de programmes et d'opérations, que l'on appelle les « *smart contracts* ». Ce système comporte cependant des risques en termes de sécurité et pose des problèmes en termes de fonctionnement centralisé d'un réseau pourtant présenté comme décentralisé, mais aussi de capacité de montée en charge. Ainsi, certaines applications sur le réseau sont susceptibles de ne plus pouvoir fonctionner lors de pics d'utilisation. Ce fut, par exemple, observé avec la première vague de « *crypto-kitties* », application de collecte et d'échanges de « chats virtuels », plus grand succès à ce jour de la *blockchain* Ethereum, mais ayant alors totalement congestionné le réseau.

M. Ronan Le Gleut, sénateur, corapporteur. – La sécurité est probablement la caractéristique des *blockchains* la plus mise en avant. En effet, il semble plus ardu de pirater un registre copié sur plusieurs milliers de serveurs disséminés à travers le monde que s'il était présent sur un unique serveur centralisé. Plus une *blockchain* possède un réseau étendu et dispersé, plus il est difficile de modifier son code ou de faire passer une transaction frauduleuse. Ces transactions frauduleuses sont bien souvent des double dépenses, permettant qu'une même somme soit dépensée deux fois.

De ce point de vue, la longévité de la *blockchain* du bitcoin semble garantir l'intégrité des transactions. Pourtant, elle n'est pas exempte de failles et a déjà été attaquée. Les autres protocoles, en particulier ceux qui développent des applications complexes, sont eux aussi exposés à des attaques. Ce risque est bien souvent croissant avec leur valeur financière : plus un système est valorisé par le marché, plus il va subir d'attaques et plus celles-ci vont mobiliser de fortes puissances de calcul.

Dans le rapport, nous avons choisi de présenter les attaques possibles en les distinguant selon quatre catégories, en fonction de la nature de leur cible.

Les attaques contre les interfaces sont les plus courantes. Elles ne portent pas sur la *blockchain* en elle-même mais sur les plateformes qui permettent à tout un chacun d'interagir avec elle, en particulier les sites internet permettant d'acheter, de vendre ou d'échanger des cryptomonnaies. Ces attaques consistent à voler les « clés privés » des utilisateurs, celles qui leur garantissent l'utilisation de leurs monnaies. Cela s'apparente à de simples vols de mot de passe mais avec des conséquences considérables. 850 000 bitcoins ont ainsi été dérobés en février 2014 sur la plateforme japonaise MtGox, ce qui équivalait alors à 660 millions de dollars. Plus récemment, en août 2016, l'équivalent de 93 millions de dollars ont été subtilisés à Bitfinex, l'une des principales « bourses » de bitcoins. Selon une estimation, un tiers des plateformes d'échange auraient ainsi été *hackées* depuis 2009.

Les attaques contre les applications vont, quant à elles, utiliser les failles de systèmes plus développés, qui prennent la forme de programmes informatiques inscrits dans la *blockchain*, les *smart contracts*. Ces derniers ajoutent de la complexité dans le protocole. Par voie de conséquence, ils ouvrent de nouvelles failles, exploitables par des attaquants, d'autant plus qu'ils ont souvent été conçus très rapidement et n'ont pas subi les tests qui prévalent à la création de logiciels plus traditionnels. Le piratage de l'application TheDAO (« *The Decentralized Autonomous Organization »),* développée sur la *blockchain* Ethereum, est probablement le plus emblématique à ce titre. Alors que ce projet très ambitieux avait réussi le tour de force de lever la somme de 150 millions d'euros sous forme de cryptomonnaie, il a été *hacké* en juin 2016. Le *hacker* a utilisé une vulnérabilité du programme pour détourner 5 % de l'ensemble des ethers en circulation. Comme vous l'a expliqué notre collègue Claude de Ganay, les ethers sont la monnaie d'Ethereum. Les conséquences de cette attaque ont toutefois été annulées grâce à un « *hard fork »*, c'est-à-dire à une modification des règles applicables à la *blockchain* elle-même.

Certaines attaques vont plutôt détourner le fonctionnement normal du protocole. Ces attaques sont d'autant plus pernicieuses qu'une *blockchain* publique ne prévoit, par définition, aucun moyen de contrôle ou de sanction.

Pour une *blockchain* qui utilise la preuve de travail, l'attaque la plus connue est celle dite « des 51 % ». Il s'agit, pour un mineur, de réunir plus de 50 % de la puissance de calcul à un instant donné afin de pouvoir valider des blocs plus rapidement que l'ensemble des autres utilisateurs. Cela lui permet alors d'effectuer des double dépenses, c'est-à-dire de réaliser plusieurs transactions avec la même unité de cryptomonnaie. Le dernier exemple qui peut être cité est celui de la *blockchain Bitcoin Gold*, dont la capitalisation dépasse les 500 millions de dollars et qui a subi une telle attaque le 24 mai dernier. De ce point de vue, la *blockchain* du bitcoin semble particulièrement sûre : au vu du nombre de mineurs, aucune double dépense ne semble suffisamment rentable au vu des moyens à investir dans une attaque 51 %. Toutefois, un gouvernement ou une organisation, qui serait prêt à investir environ 3 milliards d'euros, pourrait mener une telle attaque à la seule fin de détruire toute confiance dans le réseau bitcoin.

Enfin, bien que le code source des protocoles de *blockchain* soit en accès libre et qu'il puisse donc ainsi être facilement surveillé, une faille dans le code lui-même n'est pas inenvisageable, y compris pour les plus anciens protocoles. Ainsi, le bitcoin a été attaqué avec succès le 15 août 2010 en raison d'une erreur dans le code utilisé pour vérifier les transactions. À l'époque, cette faille n'a toutefois eu que des conséquences très limitées. Elles seraient bien plus importantes aujourd'hui. De plus, les algorithmes cryptographiques ont tous une durée de vie limitée, qui est tout de même estimée au minimum à vingt ans pour la fonction de hachage du bitcoin, SHA-256. Ces attaques contre le protocole lui-même restent néanmoins parmi les moins probables car celui-ci bénéficie de la vérification collective de développeurs dans le monde entier.

Le rôle de la *blockchain* en tant que technologie sous-jacente des nombreuses cryptomonnaies est aujourd'hui dominant. Cependant, ses protocoles se déclinent dans de nombreux autres secteurs et pourront donner naissance à des applications nouvelles variées, dépassant le cadre strict de la finance. Peuvent notamment être cités les services d'attestation et de certification (*proofs of existence*) pouvant concerner l'état civil, le cadastre, les contrats de type notarié ou encore des mécanismes de protection de la propriété intellectuelle. Une autre application pourrait être les opérations de vote, sur laquelle nous revenons dans le rapport.

Une autre catégorie d'applications est celle des *smart contracts,* programmes informatiques inscrits dans la *blockchain,* qui ne sont pas des contrats au sens juridique mais qui facilitent, vérifient ou exécutent un contrat au stade de sa négociation ou de sa mise en œuvre. Ils pourront accompagner le déploiement des objets connectés tout en garantissant la confiance dans les informations échangées entre les appareils. Cependant, la mise en œuvre de ces cas d'usage est conditionnée à l'import et l'export d'informations. Or, nous avions souligné, en avril dernier, que de tels systèmes aboutissent au retour d'un « tiers de confiance » puisque, pour relever une température, livrer un colis, prouver la réalisation d'un travail ou donner l'heure d'arrivée d'un avion, un tiers, qualifié d'« oracle » dans l'écosystème Ethereum, doit faire le lien entre la *blockchain* et le reste du monde.

Je voudrais enfin aborder les ICO, *Initial Coin Offerings*, en français *« offres initiales de monnaie »,* qui sont des formes de levée de fonds où les investisseurs échangent des cryptomonnaies contre des jetons, *tokens* en anglais. Assez proches du *crowdfunding*, ces levées de fonds, spécifiques à l'écosystème des cryptomonnaies, connaissent un succès absolument considérable. Elles ont représenté un total cumulé de plus de 8 milliards d'euros en mars 2018. Ce succès peut sembler peu rationnel puisque la possession de *tokens* n'offre aucune garantie aux investisseurs. Elles posent aussi des problèmes de transparence, d'intérêt de l'actif vendu, de spéculation, voire tout simplement d'escroqueries.

Cependant, ces ICO représentent une opportunité nouvelle pour les start-up qui évoluent dans le secteur des nouvelles technologies de l'informatique, ou *deep tech*. En effet, les moyens traditionnels de levée de fonds tels les crédits bancaires et le capital-risque (*venture capitalism*) ne répondent que rarement à leurs besoins spécifiques de rapidité et de souplesse, à la forte technicité de leurs projets et au caractère *open source* de leurs innovations.

Les projets financés sont, aujourd'hui encore, en grande partie propres au monde des *blockchains*. Certes, les ICO doivent être regardées avec prudence mais aussi sous l'angle des perspectives nouvelles de développement économique qu'elles ouvrent.

Mme Valéria Faure-Muntian, députée, corapporteure. – Comme vous avez pu le constater à travers les présentations de nos collègues Ronan Le Gleut et Claude de Ganay, nous sommes en présence d'une technologie encore assez jeune et méconnue, qui pose de vraies questions. Nous avons, en particulier, voulu soulever les enjeux énergétiques, juridiques et de souveraineté liés aux *blockchains*.

En ce qui concerne l'énergie, la preuve de travail ou POW, qui nécessite, pour les seules *blockchains* publiques, une compétition entre mineurs pour remporter une rémunération, conduit à ce que beaucoup de supercalculateurs travaillent en permanence. Cela nécessite une consommation énergétique extrêmement importante. Les *blockchains* privées, *a contrario*, nécessitent beaucoup moins d'énergie, mais nous avons vu que leur pertinence en comparaison des *blockchains* publiques est moins évidente.

Trois méthodes d'estimation de la consommation énergétique des *blockchains* peuvent être citées, sachant qu'aucun calcul exact n'est possible. Ces méthodes donnent des valeurs allant d'au minimum 46 TWh/an jusqu'à 200 TWh/an. On peut comparer ces résultats à la production électrique d'un réacteur nucléaire, qui est de 6 TWh/an, ou encore à la consommation électrique française, qui est de 530 TWh/an. La croissance de cette consommation peut d'autant moins persister que les fermes de minage se situent principalement en Chine, pays qui présente, pour sa production électrique, l'intensité carbone la plus élevée au monde.

La preuve de travail pose aussi, au-delà des questions de consommation énergétique, des problèmes de gaspillage de matériel informatique spécialisé. En effet, les supercalculateurs, qui pourraient être utilisés au bénéfice de l'innovation, de la recherche ou du test de nouvelles technologies, tournent en quelque sorte « dans le vide », exclusivement au bénéfice de celui qui emporte la mise en calculant des preuves de travail pour la *blockchain*.

Il est donc nécessaire de s'orienter vers une autre méthode de consensus que la preuve de travail. Beaucoup de projets alternatifs sont d'ailleurs envisagés, comme l'a indiqué Claude de Ganay. Néanmoins, aucun n'a encore totalement abouti en termes de sécurité. La recherche doit aider à trouver des preuves d'enjeu qui présentent le même niveau de sécurité que la preuve de travail. Sinon, au vu de l'augmentation du nombre de transactions sur les *blockchains*, on risque d'arriver à une situation critique en termes de consommation énergétique.

En ce qui concerne les enjeux juridiques, l'immuabilité et la distribution globale et ouverte de la *blockchain* interrogent forcément le législateur.

Ainsi, on a pu dire que les cryptomonnaies faciliteraient les utilisations frauduleuses et prêter, par exemple, au bitcoin une utilisation significative dans l'économie parallèle. Cela doit toutefois être relativisé au regard du poids total du crime organisé, estimé à environ 900 milliards de dollars par an.

Par ailleurs se pose la question de la responsabilité, le réseau étant distribué sans centralisation. Vers qui se tourner en cas de problème, avec quelles preuves et à qui demander réparation ? C'est une question importante.

Le régime fiscal de la cryptomonnaie pose, lui aussi, question, surtout avec les ICO qui permettent de lever des fonds importants. Quel régime fiscal leur appliquer ? C'est une question à laquelle il faut apporter des réponses.

Enfin, face au règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai dernier, on peut s'interroger sur le respect du droit de rectification et du droit à l'oubli. La *blockchain* étant immuable, un bloc ne peut plus être modifié une fois qu'il est validé par consensus. Nous avons discuté de ce point avec la CNIL, qui nous a indiqué l'existence de solutions technologiques qui permettraient d'apporter des rectificatifs, grâce à une écriture nouvelle, sans cependant réécrire les précédents blocs de la chaîne. C'est une piste mais on n'est pas dans un respect total du droit à l'effacement.

Il y a finalement une contradiction forte entre l'exigence de transparence, surtout si l'on prête à la *blockchain* le risque d'usages frauduleux par le crime organisé, et celle de l'anonymisation, qui permet de protéger les données personnelles. Il faudra trouver un compromis.

Enfin, en termes de souveraineté, et comme nous l'avons déjà souligné dans la note courte, les fermes de minage sont plutôt concentrées géographiquement, 60 % d'entre elles se trouvant en Chine. La Russie encourage, elle aussi, l'implantation de *pools* de mineurs à des fins stratégiques, notamment parce qu'elle dispose de capacités énergétiques.

Par ailleurs, la compétition entre les protocoles est très forte. Une fois que des protocoles à la consommation énergétique maîtrisée auront été trouvés, l'un de ceux-ci risque de devenir un monopole.

Nous avons constaté, à travers nos auditions, que l'idée d'une *blockchain* souveraine, contrôlée par un État, serait peu pertinente. Si l'on veut réaliser des enregistrements sécurisés, il n'est pas forcément besoin d'un registre distribué, d'autant plus que, dans ce cas, les acteurs du réseau seraient nommés par avance. Cependant, nous

souhaitons insister sur la nécessité de la recherche et du développement, à travers nos *start-up*, de technologies qui respectent les valeurs européennes liées à la protection du consommateur et aux données personnelles.

Il nous paraît important d'encourager cette technologie prometteuse des *blockchains*. Mais les usages actuels étant principalement adossés aux *blockchains* Bitcoin et Ethereum, il serait opportun de promouvoir une création d'origine européenne avec un protocole légèrement modifié pour permettre le respect de nos valeurs. Des acteurs s'y attellent et ont déjà levé des fonds à cette fin.

La Commission européenne a, il est vrai, lancé un Observatoire des *blockchains*. Mais celui-ci est géré par une organisation extérieure, l'entreprise Consensys, entreprise américaine adossée à la technologie Ethereum, qui a été choisie alors même que des acteurs français et européens existent dans ce domaine. Nous sommes déçus. Il nous semble dommage de prendre le risque d'oublier nos particularités européennes, voire notre souveraineté.

Pour conclure, les perspectives ouvertes par les *blockchains* sont considérables et ne doivent pas être ignorées. Il est nécessaire de continuer la R & D, qu'elle soit publique ou privée, voire en coopération. Les limites technologiques sont sérieuses et il faut y répondre avant de pouvoir massifier les usages. La France et l'Union européenne devront se saisir pleinement de cette technologie et en être à l'avant-garde. Puisqu'aucune législation n'a encore été mise en place dans le monde sur cette technologie, nous pourrions être précurseurs, en proposant des normes qui nous ressemblent. Je vous remercie.

M. Gérard Longuet, sénateur, président de l'Office. – Vous nous remerciez mais c'est surtout nous qui vous remercions pour ce travail collectif très impressionnant et passionnant. Il montre accessoirement toute la légitimité, non seulement de l'Office mais aussi de l'ensemble du travail parlementaire, sur ces questions. C'est un document qui fera date, sans mettre de point d'arrêt à un débat extraordinairement vivant.

M. Cédric Villani, député, premier vice-président de l'Office. – Mes chers collègues, je voudrais vous adresser mes sincères félicitations. Depuis que cette technologie des *blockchains* est apparue, j'ai eu l'occasion d'en discuter dans divers contextes, y compris dans des conférences scientifiques ou avec de grandes entreprises, mais ce rapport est, de très loin, le meilleur document que j'ai vu sur le sujet. Votre travail est remarquable et offre des réponses quantitatives à certaines questions qui n'étaient identifiées que qualitativement, telles que la consommation énergétique ou la comparaison des différentes technologies.

Ma première question porte sur la preuve de travail, qui, comme vous l'avez bien expliqué, conduit à une débauche énergétique insoutenable. Beaucoup d'alternatives sont envisagées mais j'ai l'impression que l'on revient, finalement, avec des yeux nouveaux sur un débat classique en théorie économique, qui est une question politique et sociale : sur quoi fonde-t-on la valeur de la monnaie ?

J'ai une seconde question à propos de la fiscalité et du crime organisé. A-t-on idée de la mesure dans laquelle le bitcoin pourrait, au contraire, être utilisé pour lutter contre la fraude ? En effet, il a une face sombre mais aussi une face plus claire, étant donné que ses registres sont transparents. Permettrait-il de lutter contre la fraude ou contre l'évasion fiscale ?

Et enfin, quelle pourrait être une politique de sensibilisation des acteurs pouvant être intéressés par ces technologies, que ce soit des entreprises ou la puissance publique ? Y a-t-il un travail de sensibilisation dans les ministères, ou ailleurs, pour lancer la réflexion ?

M. Stéphane Piednoir, sénateur. – Je voudrais féliciter les trois rapporteurs pour ce travail qui nous éclaire et qui nous emplit d'humilité, pour connaître un tout petit peu le sujet. Évidemment, je vais moi aussi porter beaucoup d'attention à ce rapport très complet. Le concept de « fermes de minage » est assez surprenant et pose beaucoup de questions, notamment énergétiques, mais aussi sur l'aspect irréversible de ces technologies. Et puis malgré la dimension virtuelle, il y a tout de même une réalité réelle, avec des gens qui investissent, certains qui spéculent. La volatilité du bitcoin et des autres cryptomonnaies m'interpelle.

Mme Catherine Procaccia, sénatrice, vice-présidente de l'Office. – Même avec vos explications, cela demeure tout de même quelque chose de très complexe. J'ai une interrogation sur la partie du rapport consacrée aux procédures électorales et au vote, sujets qui nous intéressent particulièrement en tant que législateurs. Je me souviens que, pour les élections de 2017, on a suspendu les élections par internet pour les Français de l'étranger car la sécurité n'était pas suffisante. Peut-être avons-nous là une technologie qui permettrait de répondre à ces questions ?

M. Claude de Ganay, député, corapporteur. – Je voudrais revenir sur un point abordé par Valéria Faure-Muntian avec beaucoup de diplomatie : le fait que la Commission européenne ait confié son Observatoire de la *blockchain* à une entreprise américaine qui devient donc juge et partie. Elle a dit que nous étions déçus, je dirais, pour enfoncer le clou, que nous dénonçons fortement un tel choix.

Mme Huguette Tiegna, députée, vice-présidente de l'Office – Je voudrais également féliciter les trois rapporteurs qui ont fait un bon travail malgré le temps court imparti. Ma première question portait sur l'observatoire européen mais Claude de Ganay vient d'aborder le sujet. Mon autre question porte justement sur l'Europe : y-a-t-il une filière qui se dessine ? Des grands groupes se structurent-ils dans ce domaine au niveau français ou européen ?

M. Ronan Le Gleut, sénateur, corapporteur. – Je vais d'abord aborder la question des alternatives à la preuve de travail, méthode qui a l'avantage d'apporter une sécurité à la chaîne de blocs mais l'inconvénient principal d'avoir une consommation énergétique que je qualifierais de folle. Je vous renvoie, pour bien comprendre, à la page du rapport où se trouvent deux photos qui représentent, pour la première, de grands hangars et, pour la seconde, ce qui se trouve à l'intérieur, c'est-à-dire des rangées multiples de processeurs : voilà ce que l'on appelle des « fermes de minage ». Ces systèmes informatiques produisent des calculs et sont inhérents au fonctionnement du bitcoin. Il y en a dans le monde entier et c'est de là que provient cette consommation énergétique.

Le problème est que cette consommation a tendance à être exponentielle, au sens commun du terme du moins. Or, comme nous sommes déjà à des niveaux très élevés, de l'ordre de 100 TWh/an, cela signifie qu'un jour, on ne pourra simplement plus produire l'énergie nécessaire au fonctionnement de la *blockchain*.

Dans le rapport, le problème initial des monnaies virtuelles est bien décrit : un utilisateur peut toujours faire semblant qu'il représente des millions d'utilisateurs avec des millions d'identités. C'est pourquoi on a besoin de ce temps de calcul, de ces exercices à résoudre, pour éviter ce problème. Ces calculs n'ont aucun but sinon de prouver qu'on est en train de faire travailler une machine, c'est le principe même de la preuve de travail.

Il s'agit du modèle de Satoshi Nakamoto, l'inventeur du bitcoin dont on ignore l'identité précise, qui l'a décrit fin 2008 dans un article fondateur, un *white paper*, qui a une valeur quasiment religieuse pour les partisans de la *blockchain* du bitcoin. Dix ans plus tard, on

constate que ce texte fondateur résout toujours la problématique de la sécurité mais, en revanche, la consommation énergétique arrive à un tel niveau qu'il devient nécessaire d'envisager d'autres solutions.

C'est ainsi qu'Ethereum, deuxième cryptomonnaie en termes de volume, indique depuis son lancement qu'elle va résoudre le problème en passant de la preuve de travail à la preuve d'enjeu. Tout le monde attend un peu ce changement, mais, annoncé depuis deux ans, il n'est toujours pas mis en œuvre, ce qui montre que cette transition soulève des problèmes techniques importants même si, depuis environ quatre mois, une nouvelle version d'Ethereum avec preuve d'enjeu est en cours de test. Pour nous, la question reste en suspens : existe-t-il véritablement une alternative viable à la preuve de travail ?

Mme Valéria Faure-Muntian, députée, corapporteure. – Concernant la participation du bitcoin au crime organisé, il est vrai que celui-ci est assez transparent en termes d'enregistrement : ce n'est pas un système anonyme mais plutôt pseudonyme. Par exemple, on a vu que la *National Security Agency* (NSA) avait les moyens de remonter certaines pistes et de faire considérablement diminuer l'usage du bitcoin dans l'économie parallèle. En revanche, il existe d'autres *blockchains*, plus petites et moins connues, pratiquement anonymes. On y a constaté une recrudescence des transactions qui pourraient être imputées au crime organisé. Évidemment, la transparence est un gage de contrôle. Cependant, en Europe, avec le RGPD, c'est un enjeu compliqué car on a aussi un besoin d'anonymisation pour la protection des données personnelles.

Concernant la fiscalité, le premier objectif est déjà de donner une existence juridique au bitcoin et à la *blockchain* qui, pour l'instant, n'existe pas. On ne peut travailler à la fiscalité des cryptomonnaies sans les qualifier juridiquement ; d'ailleurs, la qualification de « monnaie » est très contestée. Est-ce un revenu ou un placement ? C'est une monnaie qui n'a pas d'autre fondement qu'elle-même. L'Autorité des marchés financiers (AMF) travaille depuis plusieurs mois sur le sujet, et en particulier sur les ICO.

C'est aussi un marché qui, aujourd'hui, fonctionne sans aucune régulation. Ainsi, lorsque le bitcoin a connu une explosion de sa valeur, personne ne pouvait décider de fermer le marché, le temps de trouver une solution. Le choix américain a été de très peu légiférer mais de contrôler tout de même et, ainsi, de geler, par exemple, les avoirs en dollars des possesseurs de bitcoins jusqu'à ce que ceux-ci se mettent en règle. Mais ce n'est sans doute pas une solution envisageable chez nous et je ne pense pas qu'on en arrivera là.

Concernant les ICO, là encore, il est complexe de rattacher les *tokens* à telle ou telle qualification juridique. Car, finalement, on ne peut en tirer profit ; ce n'est pas un titre de propriété ni un titre obligataire : il ne rapporte pas d'intérêt et ne donne aucun pouvoir vis-à-vis de l'auteur de la levée de fonds. Le but est différent, il s'agit de donner en toute confiance, à une personne ou une entreprise, de l'argent pour développer une innovation sans rien attendre en retour d'autre que l'usage futur de cette technologie.

Ainsi, si quelqu'un veut voir émerger un jeu avec des petits chats et qu'une structure le lui propose, il peut financer ce projet sans qu'il n'y ait aucun lien d'obligation entre celui qui investit et celui qui récupère l'argent. Imposer une fiscalité sur cette opération reviendrait exactement à imposer une fiscalité sur le *crowdfunding*, et je ne sais pas où l'on en est sur ce sujet.

M. Cédric Villani, député, premier vice-président de l'Office. – Si je comprends ce qui se dégage des réponses : premièrement, le bitcoin a été introduit pour répondre à deux grands objectifs, d'abord l'infalsifiabilité, ensuite l'absence de pilote à bord. Par rapport à une monnaie étatique, le premier objectif séduit tandis que le second effraie. Il faudrait savoir si

l'on peut garder l'un de ces aspects sans toucher à l'autre, d'où des réticences des États, ce qui semble être un sujet de fond.

Deuxièmement, la *blockchain* est un principe technologique qui peut se réaliser de nombreuses façons différentes mais qui ne dit rien, au fond, de ses usages précis. La législation devrait, en revanche, s'appuyer sur des finalités données. La question est de savoir sur quoi on veut légiférer, si c'est le bitcoin en soit ou si c'est sur tel ou tel aspect, or ce n'est pas clair. Si nous devions écrire la loi demain, nous serions bien embarrassés. J'ai cru comprendre que la Chine avait légiféré sur le bitcoin ; comment a-t-elle fait ?

Mme Valéria Faure-Muntian, députée, corapporteure. – Je voudrais rappeler qu'il y a plusieurs missions parlementaires en cours : celle de la commission des finances du Sénat, celle de la commission des finances de l'Assemblée nationale et celle commune à trois commissions permanentes à l'Assemblée nationale, présidée par Julien Aubert. Ces trois missions sont censées trouver des réponses à toutes ces questions ou, en tout cas, essayer.

En ce qui concerne la législation chinoise, il est compliqué d'en connaître les justifications et les détails car il y a peu de communication dessus. En tout cas, la Chine a pris cette question au sérieux, d'abord à cause de la prolifération des fermes de minage, alors qu'elle essaie de sortir du cercle vicieux de la pollution, qui commence à faire sentir ses effets sur la mortalité dans le pays, ensuite, en raison de l'aspect totalement anarchique des usages des *blockchains*, qui ne convient pas au régime.

En effet, on peut légiférer sur beaucoup de choses mais y a-t-il un intérêt à le faire maintenant ? Peut-on imaginer une sorte de TVA sur des transactions entre un Australien et un Néo-zélandais, validées par un Chinois ? C'est compliqué à envisager et quasiment impossible à contrôler.

Je crois que, pour l'instant, il faut s'intéresser aux *blockchains* avec l'idée qu'elles ouvrent certaines possibilités inédites. En particulier, les ICO sont ce que l'on a vu de plus pertinent. Ces opérations sont souvent sans but lucratif, car les entreprises ne tireront pas toujours profit de leurs projets, et c'est généralement parce qu'elles ont du mal à se financer sur le marché bancaire classique qu'elles y ont recours.

Pour répondre à la question sur l'existence d'une filière, je dirais qu'il n'en existe pas encore, que les initiatives sont assez dispersées et que les seuls usages bien organisés pour le moment sont les *blockchains* privées. Par exemple, il existe de grands réseaux bancaires qui utilisent ces solutions. Ces *blockchains* privées ont une gouvernance qui n'a rien à voir avec la technologie ouverte des *blockchains* publiques.

Faire des profits avec des applications sur une *blockchain*, ce que tentent, par exemple, les entreprises qui travaillent sur Ethereum, ne nous a pas semblé très concluant pour le moment.

M. Gérard Longuet, sénateur, président de l'Office. – Qui investit et comment ces personnes sont-elles rémunérées pour leurs investissements ?

M. Ronan Le Gleut, sénateur, corapporteur. – Il y a un système de rémunération : lorsque la ferme de minage gagne la compétition cryptographique, elle obtient actuellement une récompense à hauteur de 12,5 bitcoins, récompense qui est décernée toutes les dix minutes. Le niveau de cette récompense est divisé par deux tous les quatre ans. À cela s'ajoutent des frais de transaction qui sont imputés à chacune des différentes transactions inscrites dans les blocs. Bien que la volatilité reste forte aujourd'hui, elle est en partie trompeuse car un graphique logarithmique montrerait que cette volatilité était beaucoup plus importante au début de la vie du bitcoin.

Sur la filière française, je voudrais indiquer que nous avons rencontré les créateurs d'une *blockchain* française, Neurochain, qui ont réussi à lever des fonds par ICO, en ayant d'abord échoué à mobiliser des fonds bancaires ou par capital-risque. Ces investisseurs classiques leur avaient expliqué que le projet était trop technique, ou plus exactement qu'ils ne le comprenaient pas. Les ICO permettent donc de toucher un public plus large qui a la capacité de comprendre l'invention. Ces mêmes créateurs ont été confrontés à un autre problème par la suite, car ils n'ont trouvé aucune banque capable de leur ouvrir un compte bancaire. Il y a là une vraie question quant à la capacité de la France à être une terre d'innovation. Si les banques françaises n'offrent pas de garanties, il n'y aura pas d'écosystème favorable en France pour ces jeunes *start-up*. C'est un vrai sujet pour le législateur, afin que nos inventeurs et entrepreneurs n'aillent pas ouvrir leur compte en banque dans un pays voisin. En l'occurrence, il ne s'agit pas d'un problème de réglementation européenne puisque d'autres banques en Europe ouvrent de tels comptes.

Mme Catherine Procaccia, sénatrice, vice-présidente de l'Office. – Mais ces comptes sont-ils ouverts en euros ou en cryptomonnaies ?

M. Ronan Le Gleut, sénateur, corapporteur. – Les cryptomonnaies peuvent être échangées sur un marché de change, elles sont donc convertibles. La plateforme Kraken, par exemple, rend ce service. On est typiquement, actuellement, dans une sorte de *Far West* de l'innovation. Il est donc normal qu'il y ait beaucoup d'incertitudes sur ces *start-up* car il faut tester les nouveaux produits ou services pour voir ce qui va fonctionner. Il faut néanmoins que la France se positionne pour offrir un environnement favorable à ces inventeurs et qu'ils puissent développer leurs activités.

Sur la question de la souveraineté, il a été rappelé qu'effectivement plus de 60 % de la puissance de calcul du bitcoin se trouve en Chine, ce qui soulève une vraie question car nous savons tous que le pouvoir chinois est capable de prendre la main sur ces usines.

Sur le vote électronique, on a effectivement abordé le sujet dans le rapport, en évoquant un certain nombre d'exemples, en Estonie ou en Colombie, qui ont donné satisfaction. Je pense qu'il faut encore regarder ces innovations avec une certaine prudence car il n'y a pas vraiment encore de maturité technologique. Dans ce domaine, il vaut mieux utiliser des technologies matures et qui ont fait leurs preuves.

D'une manière générale, face à ce type de technologies nouvelles, il faut faire attention à ne pas aller vers l'écueil d'un excès de réglementation, l'innovation ayant besoin de liberté pour être créative.

Mme Valéria Faure-Muntian, députée, corapporteure. – Pour revenir à la réglementation et à l'ouverture de comptes en banque, ce qui pose problème, c'est la réglementation TRACFIN. Les banques refusent d'ouvrir des comptes car elles ne savent pas d'où vient l'argent. Cette exigence de traçabilité explique ce refus systématique. Il faudrait trouver un moyen pour que l'argent puisse être utilisé, en assurant sa traçabilité, ce qui démontrerait, par exemple, qu'il ne provient pas du crime organisé.

En ce qui concerne la diffusion de l'information sur cette technologie, il faut savoir qu'il y a des chercheurs, des *start-up*, des PME et, même, dans une certaine mesure, des grandes entreprises qui travaillent sur le sujet. Il faut trouver la voie d'une collaboration étroite entre le secteur public et le secteur privé afin d'utiliser cette technologie sans tomber dans l'effet de mode, mais de manière à ce qu'elle apporte, pour le consommateur comme pour les entreprises, des solutions pérennes.

M. Cédric Villani, député, premier vice-président de l'Office. – Merci pour toutes ces explications. Sur la question des banques, il est paradoxal d'observer que des grandes banques investissent beaucoup dans la recherche sur les technologies autour du bitcoin mais n'ouvrent pas de comptes aux *start-up* agissant dans ce domaine !

M. Gérard Longuet, sénateur, président de l'Office. – Je vous propose de féliciter à nouveau nos rapporteurs, d'autoriser la publication de ce rapport et de mobiliser nos services, à l'Assemblée comme au Sénat, pour assurer la notoriété de celui-ci.

La publication du rapport sur les enjeux technologiques des* blockchains *(chaînes de blocs) est autorisée à l'unanimité.

COURRIER DE LA MISSION D'INFORMATION COMMUNE DE L'ASSEMBLEE NATIONALE SUR LES *BLOCKCHAINS*

ASSEMBLÉE NATIONALE

RÉPUBLIQUE FRANÇAISE
LIBERTÉ – ÉGALITÉ – FRATERNITÉ

COMMISSION DES AFFAIRES ÉCONOMIQUES
COMMISSION DES FINANCES
COMMISSION DES LOIS

MISSION D'INFORMATION COMMUNE SUR LES BLOC-CHAINES

M. Cédric Villani
Député de l'Essonne
Premier vice-président de l'OPECST

Paris, le 19 février 2018

Monsieur le premier vice-président, *C. Villani*,

Mme Laure de la Raudière et M. Jean-Michel Mis, rapporteurs, se joignent à moi pour vous remercier de l'attention que vous portez aux travaux de la de la mission d'information commune sur les bloc-chaînes.

Nous sommes très sensibles à l'offre que vous nous faites de contribuer à ces travaux par un éclairage des enjeux technologiques et numériques de la bloc-chaîne. Si vous jugez possible de produire une contribution dans des délais compatibles avec le calendrier de la mission (de six à sept mois), nous serions particulièrement intéressés par un état des lieux comparatif des technologies de la bloc-chaîne, de leurs mérites et de leurs limites ou défauts respectifs, notamment en termes de performance, de sécurité ou de consommation énergétique.

Nous nous tenons évidemment à votre disposition pour échanger sur les modalités de la contribution que l'Office pourrait apporter à la mission, tant sur le plan formel que sur le fond.

Je vous prie d'agréer, Monsieur le premier vice-président, l'expression de ma considération distinguée.

Julien Aubert
Député de Vaucluse
Président de la mission