Total Record

Guillaume Helleu, Anthony Masure

TOTAL RECORD

Les protocoles blockchain face au post-capitalisme

Guillaume Helleu, Anthony Masure

Association Multitudes | « Multitudes »

2018/2 n° 71 | pages 70 à 79

ISSN 0292-0107

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-multitudes-2018-2-page-70.htm

Total Record
Les protocoles blockchain face au post-capitalisme

Guillaume Helleu & Anthony Masure

Adaptation de la nouvelle de science-fiction de Philipp K. Dick « Souvenirs à vendre[1] » (1966), le long-métrage *Total Recall* de Paul Verhoeven (1990) met en scène une corporation tyrannique exploitant les ressources minières martiennes. Rêvant fréquemment de la planète Mars alors même qu'il ne s'y est jamais rendu, un être humain, Douglas Quaid (dénommé Quail dans la nouvelle), se voit proposer par la société Rekal Inc. l'implantation de faux souvenirs de voyage dans son cerveau. La mémoire humaine devient un disque dur qui peut être réécrit (reprogrammé) depuis l'extérieur sans que celle-ci ne soit consciente des traces de cette manipulation. Dans le film de Verhoeven, Quaid part sur Mars pour tenter de découvrir sa véritable identité. À l'inverse, dans la nouvelle, il fait le choix de se rendre aux forces d'Interplan et préfère sauver sa vie en effaçant définitivement son passé d'agent secret pour ne pas céder sur son désir[2]. Cette fiction interroge directement la nature fluctuante du psychisme humain : « Si vous étiez vraiment allé sur Mars comme agent d'Interplan, à l'heure actuelle vous auriez oublié la quasi-totalité de votre mission ; nos analyses […] démontrent qu'une foule de détails s'évanouissent très rapidement. Et définitivement. Dans le contrat global que nous [Rekal Inc.] offrons, les souvenirs sont si profondément implantés que rien n'est oublié.[3] »

1 Philipp K. Dick, « We Can Remember It for You Wholesale » [« Souvenirs à vendre »], *Fantasy & Science Fiction*, avril 1966. Trad. de l'américain par Hélène Collon, dans *Total Recall et autres récits*, Paris, Folio SF, 2018.

2 Le gérant de Rekal Inc., McLane, en vient ainsi à constater que des fragments mémoriels de Quail ont résisté à la reprogrammation : « Ils n'ont pu effacer cela ; ce n'est pas un souvenir mais un désir […]. » « Souvenirs à vendre », *op. cit.*, p. 230.

3 *Ibid.*, p. 224.

Mort à crédit

Le cauchemar psychotique de la nouvelle de K. Dick préfigure de façon inquiétante le développement des réseaux d'information, et plus particulièrement leur faculté à opérer à échelle globale des mécanismes de surveillance voire d'aliénation des populations. Dépassant les dystopies des séries d'anticipation, des entreprises chinoises (Alipay et WeChat) notamment spécialisées dans le paiement mobile, attribuent depuis 2013 à leurs utilisateurs une note de crédit à trois chiffres. Parallèlement, le gouvernement chinois a mis en place depuis 2014 un score social (« *social credit* ») censé mesurer la « réputation » des citoyens, entreprises ou organismes nationaux, et dont la généralisation est prévue pour 2020[4]. Dès lors que les GAFAM, les banques et les grandes entreprises occidentales évaluent également (et depuis longtemps) leurs partenaires et clients, la prolifération des données (*big data*) et leur collecte industrialisée (traqueurs, capteurs, etc.) rendent désormais possible le fantasme d'un enregistrement global et totalitaire (« *total record* ») faisant migrer les centres de pouvoir gouvernementaux vers des entreprises privées (*data is power*). Face à cette *centralisation* des écritures fiduciaires, les protocoles blockchain apparus à partir de 2009 permettent au contraire d'enregistrer de façon *distribuée* des données numériques via des technologies d'écriture théoriquement infalsifiables. Pointe avancée du capitalisme spéculatif pour certains[5], ces derniers ne seraient ainsi qu'une énième dérive de la finance néolibérale. Pourtant, l'étude du fonctionnement technique singulier de ces architectures d'informations ne nous invite-t-elle pas *également* à interroger la confiance placée dans les actuelles (et centralisées) instances du pouvoir[6] ? Autrement dit, pourrait-on prendre de vitesse les excès du capitalisme en s'appuyant sur les technologies ayant permis son renouvellement ?

Le crypto-anarchisme et les prémices des monnaies électroniques

Face à la surveillance généralisée du Web (et du monde en général), la communauté *cypherpunk* (« crypto-anarchiste ») née dans les années 1980 a vite compris que l'alliance des États et des banques faisait planer le spectre d'une réduction drastique des libertés individuelles, bien loin des utopies de liberté qui existaient aux débuts des réseaux d'information[7]. L'enregistrement (*record*) des activités humaines dans des bases de données centralisées et contrôlées par des États rejoint directement les inquiétudes pointées par K. Dick dans sa nouvelle. Vers la fin de cette fiction, un policier d'Interplan s'adresse à Douglas Quail, dont les incohérences psychiques dues à la « programmation de souvenirs artificiels » menacent de

4 Mara Hvistendahl, « Inside China's Vast New Experiment in Social Ranking », *Wired*, 14 décembre 2017, www.wired.com/story/age-of-social-credit

5 Pascal Ordonneau, « L'économie du Bitcoin devient pire que celle des subprimes », *Les Échos*, 22 septembre 2017.

6 Philippe Rodriguez, *La Révolution Blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, Paris, Dunod, 2017.

7 Fred Turner, *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence* [2006], trad. de l'anglais par Laurent Vannini, Caen, C&F, 2012.

révéler son passé d'agent secret : « Tout ce que vous pensez pourra être retenu contre vous […] Mais ça n'a plus d'importance maintenant ; à cause de ce que vous avez pensé, de ce que vous avez exprimé, vous vous êtes d'ores et déjà condamné à l'oubli[8]. » Afin de lutter contre la volonté des gouvernements de réduire voire d'interdire le chiffrement des données numériques (ce qui permettrait entre autres de résister à l'inscription d'opinions politiques dans des registres surveillés), l'informaticien David Chaum propose dès 1983 le concept d'une monnaie électronique anonyme et intraçable[9]. Ce courant de pensée à la frontière entre anarchisme et libertarianisme (rejet d'un pouvoir lointain, régenteur et archi-centralisé) rejoint les ambivalences des actuelles luttes *post-capitalistes* : se servir des stratégies d'expansion du capitalisme permettrait de dépasser sa logique délétère. Les crypto-anarchistes vont utiliser les techniques du capitalisme de surveillance (celles de l'enregistrement de données), mais en y ajoutant un *chiffrement* rendant « illisibles » les informations, qui deviennent dès lors, tout comme les rêveries des nouvelles de K. Dick, particulièrement retorses à contrôler. L'idéal d'émancipation énoncé par David Chaum est prolongé par l'informaticien Timothy C. May, qui déclarait en 1992 que « tout comme la technologie de l'imprimerie a altéré et réduit le pouvoir des corporations médiévales et la structure sociale de pouvoir, les techniques de chiffrement changeront fondamentalement la nature de l'interférence du gouvernement et des grandes entreprises dans les transactions économiques[10] ». Un an plus tard, le mathématicien Eric Hughes mettra encore davantage l'accent sur la relation entre l'émancipation collective et le chiffrement monétaire : « Nous, les cypherpunks, sommes dévoués à construire des systèmes garantissant l'anonymat. Nous défendons notre vie privée avec la cryptographie […], avec des signatures numériques, et avec une monnaie électronique.[11] »

De la crise des *subprimes* au protocole Bitcoin

Pourtant, tout comme les monnaies locales, l'idée d'une monnaie électronique échappant au système bancaire ne se concrétise vraiment qu'au tournant de la crise des *subprimes* de 2007 et des faillites bancaires de 2008, qui mirent en évidence – si besoin – l'illusoire moralisation d'un capitalisme autophage : les *derivatives* (« produits dérivés ») représenteraient actuellement entre 544 billions (mille milliards) et 1,2 quadrillion (un million de milliards de milliards) de dollars, soit donc bien davantage que l'ensemble des bourses mondiales ou que l'ensemble des devises en circulation. Tout comme le bitcoin, le dollar est donc en grande partie « numérique » : seul moins de 10 % de l'argent accessible (*narrow money*[12]) existerait sous une forme physique

8 *Ibid.*, p. 239.

9 David Chaum, « Blind Signatures for Untraceable Payments », dans : *Advances in Cryptology*, Boston, Springer, 1983, http://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

10 Timothy C. May, « The Crypto Anarchist Manifesto » [1988], texte lu par l'auteur au *Cypherpunk Meeting* de septembre 1992, www.activism.net/cypherpunk/crypto-anarchy.html Trad. des auteurs.

11 Eric Hughes, « A Cypherpunk's Manifesto », mars 1993, https://activisme.fr/cypherpunk/manifesto.html Trad. des auteurs.

12 Masses monétaires M0 et M1. Voir : « Narrow Monney », *Investopedia*, www.investopedia.com/terms/n/narrow-money.asp

– cette tendance s'étant considérablement accentuée depuis la fin des accords de Bretton Woods en 1971 (le dollar était auparavant indexé sur l'or) [**fig. 2**]. Valeur la plus connue des *crypto-actifs* (expression désormais employée par le législateur), le protocole Bitcoin et sa monnaie éponyme, (le bitcoin, avec un « b » minuscule) ont été rendus publics en 2009 sous le pseudonyme de Satoshi Nakamoto, dont l'identité comme individu ou groupe reste à ce jour encore sujette à spéculation. La filiation avec le mouvement crypto-anarchiste est clairement annoncée dans la première transaction bitcoin (*genesis block*) datant du 3 janvier 2009, qui reprend – d'une façon probablement ironique – la une du quotidien *Times* du même jour indiquant que « le ministre des finances [britanniques] est sur le point de renflouer une deuxième fois les banques[13] ».

Bitcoin aujourd'hui : le triomphe de la spéculation ?

Bitcoin a par la suite été en grande partie récupéré par un capitalisme spéculatif peu soucieux de l'idéologie anarchiste qui le sous-tendait. Inventeurs malheureux du concept d'annuaire universitaire ConnectU (Harvard) qui fut plagié par le développeur Mark Zuckerberg à l'origine de TheFacebook (2004), les frères Winklevoss ont par exemple acheté massivement des bitcoins dès 2013 via leur fond de capital-risque[14]. Passé de 0,00071 euro en 2009 à quelque 6 500 euros en mars 2018 après un pic à 16 000 autour de noël 2017, le bitcoin n'apparaît dans les *mass médias*, la plupart du temps, que sous l'angle de son utilisation à des fins frauduleuses (*ransomwares*, drogues, etc.), de la spéculation financière, ou de la pollution énergétique. L'étude de son fonctionnement technique singulier permet pourtant d'entrevoir d'autres finalités que celles du retour sur investissement. Bitcoin est *aussi* utilisé à des fins sociales par des personnes exclues des services bancaires[15], qui représentent près de deux milliards de personnes à l'échelle mondiale : ces individus à la marge économiquement « pourraient » devenir leur propre banque.

Un registre de transactions public et décentralisé

Au niveau technique, Bitcoin actualise le principe séculaire du registre financier (*bank record*) au regard des techniques cryptographiques (*arbre de Merkle*, fonction de *hachage*, *chiffrement asymétrique*, etc.) et de la décentralisation propre à Internet (architecture *client/serveur*). Bitcoin prend ainsi la forme d'un livre de compte analogue à un registre bancaire, mais distribué (non centralisé) et partagé en ligne. Incrémentable par tous les nœuds du réseau, le registre Bitcoin est partagé en *peer-to-peer* (pair à pair) [**fig. 3**]. Le protocole Bitcoin se résume à un enregistrement des transactions des *unités-bitcoins* faites sur le réseau, c'est-à-dire aux transferts de « propriété » de bitcoins d'une entité à une autre. Ce mécanisme rend

13 « Genesis block », BitcoinWiki, https://en.bitcoin.it/wiki/Genesis_block

14 Cameron Winklevoss, « Bitcoin: The Internet of Money », *Winklevoss Capital*, septembre 2013, https://winklevoss-capital.com/value-investors-congress-presentation

15 Laurence Allard, « Le bitcoin s'adresse aussi aux exclus du système bancaire », *L'Humanité*, décembre 2017, https://humanite.fr/laurence-allard-le-bitcoin-sadresse-aussi-aux-exclus-du-systeme-bancaire-647243

par conséquent impossible, contrairement à l'économie de la dette, l'obtention de soldes négatifs. Comme la plupart des monnaies « traditionnelles » (dites « fiduciaires », FIAT), la seule « matérialité » des bitcoins réside dans un registre, à la différence que le registre Bitcoin n'est pas une représentation de valeur mais *est* la valeur même : ces bitcoins n'existent donc que sous la forme de leur inscription dans la blockchain. La mention de personnes ayant « perdu » des bitcoins stockés dans des disques durs ou clés USB est un abus de langage : ce sont en réalité des « clés privées » (codes d'accès) qui ont été égarées, et sans lesquelles les utilisateurs ne peuvent pas s'authentifier sur le réseau. On estime qu'entre 2,8 et 3,8 millions de bitcoins (soit un peu moins de 20 % des unités disponibles) ne peuvent plus être récupérés et sont donc définitivement « figés » dans la blockchain.

Fonctionnement des chaînes de blocs

Les transactions Bitcoin ne sont pas enregistrées les unes après les autres, mais « page par page », dans des blocs contenant un ensemble de transactions validées par le réseau à un instant T [**fig. 1**]. La main-d'œuvre permettant de valider et d'inscrire ces « chaînes de blocs » (*blockchain*) est constituée de « mineurs ». Un mineur (ou « nœud ») est une personne qui contribue au réseau Bitcoin en téléchargeant le logiciel-registre *open source* et en y allouant de la puissance de calcul issue de son ordinateur. Ces mineurs sont chargés de mettre à jour le registre en validant et en écrivant les nouveaux blocs comprenant les nouvelles transactions. Sans cette main-d'œuvre, le protocole disparaît. Les mineurs peuvent à chaque instant soumettre au réseau (aux autres mineurs) leur version du nouveau bloc à insérer dans le registre. Pour écrire leur « page », les mineurs vont sélectionner au sein de la *memory pool* (mémoire temporaire), qui comprend les transactions en attente soumises par les utilisateurs, celles qu'ils souhaitent inclure dans leurs blocs. Ces dernières étant classées par frais de transactions, celles contenant les frais les plus élevés seront sélectionnées en premier.

Un consensus algorithmique

Les versions d'un nouveau bloc pouvant varier d'un mineur à l'autre, le protocole doit donc faire appel à un « consensus ». Celui de Bitcoin repose sur la technologie du *Proof-of-Work* (« validation par preuve de travail »)[16], qui oblige le mineur à faire « valider » son bloc avant de le soumettre. Ce dernier doit pour cela exercer une sorte de « transformation » du bloc, appelée « opération de hachage ». Une fonction de *hachage* (sur Bitcoin SHA256) permet de transformer n'importe quelle donnée numérique en un produit (suite de caractères alphanumériques) appelé « hash » constituant une « empreinte » (ou « condensat cryptographique ») de la donnée initiale. Cette opération est irréversible et permet de vérifier si une donnée spé-

16 Avec la multiplication des *cryptos-actifs*, de nombreuses variantes de consensus algorithmiques ont été développées : Ethereum, par exemple, travaille à l'implémentation du *Proof-of-Stake* qui permettrait une diminution significative de la consommation énergétique ainsi qu'une rétribution moins partiale des mineurs. Le protocole NEO, avec le *Delegated Byzantine Fault Tolerance* (dBFT), empêche tout *fork* de la blockchain.

cifique correspond bien à son *hash* (toute modification de cette dernière produisant un *hash* différent). Cet exercice consiste à trouver de manière itérative un nombre (*nonce*) intégré au nouveau bloc, de telle manière que cela produise un résultat *(hash)* respectant certaines caractéristiques prédéfinies par le réseau. La difficulté de cette opération, qui ne dépend que de la puissance de calcul et du temps alloué au réseau, est automatiquement ajustée au regard de la puissance totale cumulée. Si ce travail de minage n'est pas indispensable au fonctionnement du protocole Bitcoin, il est pourtant primordial pour garantir sa sécurité en raison du coût énergétique et financier que nécessiterait une éventuelle fraude ou attaque du système.

Mineurs et chasseurs de prime

Le mineur qui aura réussi à soumettre sa version du bloc gagne tous les « frais de transaction » associés à celle-ci par les utilisateurs, mais ce dernier sera également – et surtout – rétribué par le protocole Bitcoin qui va lui attribuer des unités (bitcoins) nouvellement créées. La récompense automatique (*block reward*) est la seule et unique manière dont les bitcoins sont créés. Cette création monétaire (*transaction coinbase*) a la particularité d'être *désinflationniste*: la rétribution en bitcoins diminue par paliers au fur et à mesure que le nombre de blocs augmente. Cette déflation continuera jusqu'à l'émission du dernier bitcoin qui devrait avoir lieu autour de 2140, pour arriver alors au nombre arbitraire et fini de 21 millions de bitcoins. En avril 2018, date d'écriture de cet article, 17 millions de BTC ont déjà été minés. Ces caractéristiques techniques valent aux bitcoins d'être – à raison – comparés à l'or : on peut en estimer les stocks, la réserve minière encore disponible, et la capacité d'extraction annuelle.

Anonymat partiel et authentification

Du point de vue des utilisateurs, la blockchain Bitcoin n'enregistre que des transactions de type A —> B. Contrairement aux institutions bancaires qui authentifient le client grâce à son identité civile (nom, prénom, date de naissance, adresse, etc.), Bitcoin opère une *pseudonymisation* des individus. Cet anonymat *partiel* (contrairement aux idées reçues) fonctionne à l'aide d'une paire de « clés » (*publique* et *privée*) basée sur une technologie cryptographique appelée *chiffrement asymétrique.* Ces deux clés, intimement liées entre elles, vont pour l'une (clé privée) permettre de chiffrer et de soumettre une demande de transaction par l'utilisateur au réseau, et pour l'autre (clé publique) de vérifier par le réseau l'authenticité de la requête.

Ethereum : applications distribuées, contrats intelligents et jetons de valeurs

Si Bitcoin concentre l'attention médiatique, ce dernier n'est pourtant que l'un des 1 500 *cryptos-actifs* qui se sont développés depuis son lancement en 2009, et dont certains se distinguent particulièrement sur le plan technique. Développée par le russo-canadien Vitalik Buterin, la plateforme Ethereum, (2015) propose ainsi de nouveaux protocoles comme les

smart-contracts (« contrats intelligents » au déclenchement automatisé), les *dApps* (« applications décentralisées » non soumises à la captation des *app stores*), les *ICOs* (« *Initial Coin Offering* », levées de fonds participatives) et les *tokens* (génération de jetons multi-usages de valeurs). Si Ethereum était à l'origine pensé comme une mise à jour de Bitcoin, les difficultés d'implémentations et de gouvernance ont poussé son inventeur à créer sa propre blockchain (Ethereum) avec sa monnaie dédiée (l'ether), qui sert avant tout à payer l'utilisation des différents services proposés par la plateforme.

Chronopolitique des *smart-contracts*

Concept inventé par le crypto-anarchiste Nick Szabo en 1993, les *smart-contracts* ne se sont vraiment développés que sous l'impulsion d'Ethereum. En permettant d'embarquer toutes sortes de métadonnées dans la blockchain, ces derniers permettent d'automatiser des actions prédéfinies par les parties ayant mis en place le contrat, comme par exemple le remboursement d'un billet d'avion dont le vol a été annulé [**fig. 4**]. Pour ce faire, il suffira au voyageur d'acheter (avec des ethers) son billet sur l'application décentralisée (*dApp*) de la compagnie aérienne concernée. Ce dernier pourra être matérialisé par un *token* (jeton-billet) spécialement conçu à cet effet. Les fonds récoltés par l'application seront bloqués par le biais d'un *smart-contract*. Cette même *dApp* sera, au moyen d'un service « Oracle » (chargé d'entrer des données extérieures dans la blockchain), connectée au réseau de l'aéroport, et déclenchera automatiquement via le *smart-contract* une action spécifique définie par le contrat. Si ces cas du quotidien généralement compliqués à régler sont désormais solvables en quelques minutes grâce à ces *smart-contracts*, d'autres usages plus politiques sont également possibles : versement d'aides sociales, rétribution égalitaire de tâches au sein d'un projet collectif (film, ouvrage, etc.), revente d'un surplus d'énergie autoproduite, etc. S'ajoute à cela la possibilité, pour n'importe qui, d'émettre des jetons (*tokens*) pouvant représenter de la monnaie ou toute autre valeur infalsifiable (vote, place de concert, item d'un jeu vidéo, part d'un bien immobilier, propriété intellectuelle, etc.[17]). Si nos actuels modes de vie sont économiquement rythmés par des temps journaliers, hebdomadaires ou mensuels, quelles seraient les conséquences humaines de contrats (débit ou crédit) exécutables à la milliseconde (salaires, factures, etc.) ? Des domaines comme les assurances, les administrations, l'énergie, les transports, les médias, etc. pourraient être considérablement transformés[18] par ces *chronopolitiques*[19].

17 Yorick de Mombynes, Gonzague Grandval, *Bitcoin, totem et tabou. Que présage l'essor des cryptomonnaies ?*, rapport de l'Institut Sapiens, février 2018, www.institutsapiens.fr/bitcoin-totem-et-tabou

18 Blockchain Partners, *La blockchain décryptée. Les clefs d'une révolution*, livre blanc, 2016, https://blockchainfrance.net/decouvrir-la-blockchain/la-blockchain-decryptee-les-clefs-dune-revolution

19 Cette idée d'un temps-argent est au centre du long métrage dystopique *Time Out* (Andrew Niccol, 2011) où l'argent, remplacé par du temps de vie, nous amène à travailler pour vivre et accélérer sa mort en dépensant.

Hacker le capitalisme protocologique

Dès lors que les usages des chaînes de blocs débordent largement du cadre monétaire, rien n'interdit *a priori* de se saisir des protocoles blockchain pour repenser l'architecture des instances de pouvoir que ces derniers tendent à révéler. Reste à savoir ce qu'engage cette notion de *protocole*. Le chercheur en théorie des médias Alexander R. Galloway[20] a montré que les systèmes électroniques décentralisés ne s'opposent pas aux « sociétés de contrôle » dénoncées par Gilles Deleuze : les gouvernements disciplinaires ont été remplacés par des *protocoles techniques* à la localisation fuyante et au *management* « distribué ». De nombreux problèmes demeurent pour rendre humainement soutenables les technologies blockchain : l'anonymat complet n'y étant (dans l'ensemble) pas garanti, le risque d'un *enregistrement global* où rien ne pourrait être oublié serait socialement très problématique. Le développement de chaînes de blocs *privées* (où les nœuds du réseau sont limités et contrôlés) pourrait de plus mettre à mal l'idée originelle de se passer des « tiers de confiance ». Reste également en suspens l'aspect énergétique, dont nul ne sait pour le moment ce qu'il adviendrait en cas d'adoption massive des protocoles blockchain – la pollution étant en l'occurrence déjà constitutive de nos sociétés de la croissance, et ce d'une manière exacerbée concernant l'actuel système financier[21].

Des scénarios *post-capitalistes* nécessiteront donc tout d'abord une prise de conscience critique vis-à-vis des effets de mode (*blockchain washing*[22]) des technologies blockchain, et ne pourront émerger qu'à condition préalable, mais non suffisante, de la technique et de la matérialité qui les sous-tendent. C'est pourquoi il s'agit moins de chercher de nouvelles armes que de déconstruire (*hacker*) les strates techniques et sémantiques des protocoles blockchain afin d'en faire des « médias tactiques » : exploiter les *failles* de cette standardisation universelle pour faciliter l'émergence d'une société plus libre et plus démocratique. Si « toute architecture d'un réseau est politique[23] », l'émergence de futurs post-capitalistes ne résidera pas dans la destruction des protocoles mais dans la capacité à *hypertrophier*[24] leurs potentiels pour inventer de nouveaux modes de vie – ou à défaut pour en démontrer les impasses.

Remerciements : Brice Genre, Frédéric Jouvin, Xavier Mouton-Dubosc, Alexandre Saint-Jevin, Adrian Sauzade,

20 Alexander R. Galloway, *Protocol. How Control Exists after Decentralization*, Cambridge, MIT Press, 2004. Trad. des auteurs.

21 « One Day, the Stock Market Could Eat the Power Grid », *Wired*, décembre 2011, www.wired.com/insights/2011/12/stock-market-power

22 Ashton Kemerling, « No, You Probably Don't Need a Blockchain », *Ashtonkemerling.com*, février 2018, http://ashtonkemerling.com/blog/2018/02/21/no-you-probably-dont-need-a-blockchain

23 *Ibid.*, p. 245.

24 *Ibid.*, p. 176 : « Techno-resistance is not outside protocol but at its center. Tactical media propel protocol into a state of hypertrophy, pushing it further, in better and more interesting ways. »

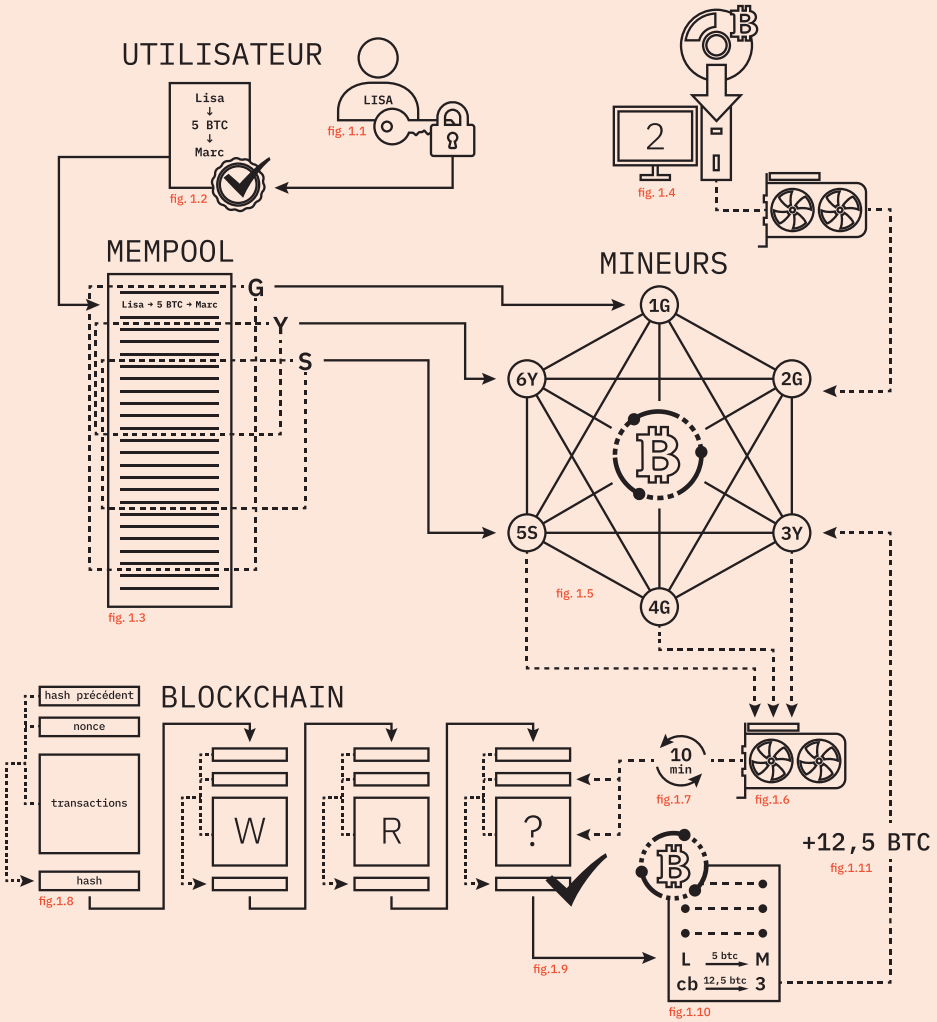

Fig. 1 : Fonctionnement technique du protocole Bitcoin. Pour envoyer 5 bitcoins à Marc, Lisa va utiliser sa clé privée [fig. 1.1] pour signer sa transaction [fig. 1.2] qui sera mise en attente dans la *mempool* [fig. 1.3]. Les mineurs [fig. 1.5] ayant préalablement téléchargé le logiciel-client Bitcoin et alloué leur puissance de calcul au protocole [fig. 1.4] vont sélectionner parmi la *mempool* les transactions à insérer dans leur version du bloc à miner. Le premier mineur qui validera son bloc pourra le soumettre au réseau et deviendra, parmi toutes celles proposées (G, Y ou S), celui qui fera foi pour soumettre un nouveau bloc. Pour ce faire le mineur va devoir « hacher » son bloc pour trouver, à l'aide d'un *nonce*, un *hash* valide [fig. 1.8]. La difficulté de cette opération est calculée au regard de la puissance totale du réseau [fig. 1.6] pour que celle-ci prenne en moyenne 10 minutes [fig. 1.7]. Une fois le bloc *miné*, celui-ci est inséré dans la *blockchain* [fig. 1.9] et permet dès lors à Lisa de voir sa transaction inscrite dans le registre [fig. 1.10]. Le mineur (3), pour avoir miné le bloc, est rétribué par une *transaction coinbase* [fig. 1.10] qui lui attribue, en plus des frais de transaction déjà gagnés, 12,5 bitcoins nouvellement créés par le protocole (taux appliqué jusqu'en 2020 avant d'être réduit à 6,25) [fig. 1.11].

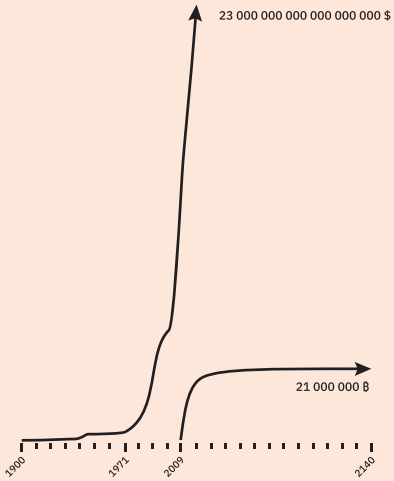

Fig. 2 : Les accords de Nixon en 1971 ont été suivis d'une hyper inflation du dollar (émission multipliée par 57 entre 1970 et 2018). *A contrario* de ce développement exponentiel, l'émission des bitcoins suit une courbe logarithmique pour atteindre le nombre maximal de 21 millions de bitcoins émis.

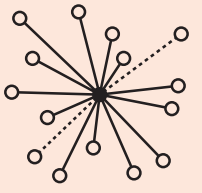
fig. 3.1

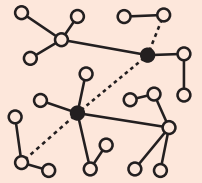
fig. 3.2

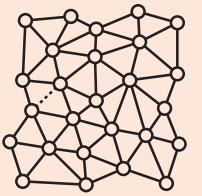
fig. 3.3

Fig. 3 : Différents systèmes d'interrelations : *centralisé* [fig. 3.1] (ex. : Paypal, Western Union), *polarisé* [fig. 3.2] (système bancaire actuel), *distribué* [fig. 3.3] (Bitcoin). On remarquera que seul ce dernier ne fait pas appel à un tiers de confiance (points noirs) pour fonctionner.

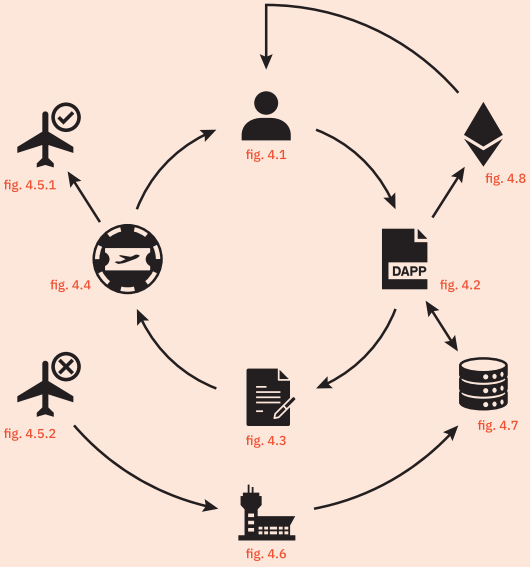

Fig. 4 : L'utilisateur [fig. 4.1] va envoyer des ethers à l'application décentralisée (*dApp*) de la compagnie aérienne [fig. 4.2] qui va enregistrer la transaction dans un *smart-contract* [fig. 4.3] et créer un token-billet [fig. 4.4]. Ce jeton sera dépensé (détruit) lors de son utilisation [fig. 4.5.1]. Si le vol est annulé [fig. 4.5.2] un *oracle* [fig. 4.7] connecté au réseau de l'aéroport [fig. 4.6] déclenchera le *smart-contract* qui remboursera, au travers de la *dApp* [fig. 4.2], l'utilisateur en ethers [fig. 4.9].