L'argent liquide digital. Le futur antérieur des cryptomonnaies ?

David Pucheu

L’argent liquide digital

Le futur antérieur des cryptomonnaies ?

David Pucheu

(Version auteur)

Version auteur. Cet article a été initialement publié dans Réseaux 2023/2 (N° 238-239), pages 45 à 74. Éditions La Découverte.

ISSN 0751-7971. ISBN 9782348079092. DOI 10.3917/res.238.0045

Depuis leur irruption dans le système économique mondial en 2008, les cryptomonnaies déchaînent les passions. Illusoire promesse pour les uns, irréversible révolution pour les autres, leur devenir reste à ce jour encore très prospectif et il serait périlleux de présumer, comme le font les « crypto-évangélistes » américains de la blockchain (Becker, 2018), quelle place elles occuperont demain dans notre écosystème mondial. Si leur usage commercial reste encore très marginal, elles ont fondamentalement participé jusqu'à présent à démocratiser la spéculation financière auprès de millions d'utilisateurs rivés sur leurs écrans à observer les courbes fluctuantes et volatiles du cours de leurs « crypto-actifs ».

En arrière-plan des cryptomonnaies et de la blockchain, initialement basées sur la puissance distribuée des ordinateurs individuels, s'est déployé un colossal agencement technique planétaire aux dimensions industrielles. Les protocoles cryptographiques s'articulent aujourd'hui autour de gigantesques fermes d'ordinateurs dédiées au « minage » où des agents humains, engagés dans une féroce compétition pour valider aveuglément des transactions, tentent d'obtenir en retour une gratification financière (opération qui conditionne l'émission de nouvelles cryptomonnaies au bénéfice de ces « mineurs »). Sorte de banques aveugles à elles-mêmes, les blockchains assurent de leur côté l'inscription et le chaînage de ces mêmes transactions dans des registres publics distribués et immuables empêchant toute possibilité de falsification ou de « double dépense ».

La confusion entretenue par cette complexité technique et sa dilution dans l'abstraction du capitalisme financiarisé dissimulent l'une des idées fondamentales qui a présidé à l'émergence des cryptomonnaies : la création d'une forme inédite d'argent liquide digital, « *e-Cash* » comme le titrait le livre blanc du bitcoin publié en 2008 par son mystérieux inventeur Satosh Nakamoto. Le récent ouvrage de Fin Brunton, *Digital Cash* (2020), éclaire cette genèse à partir des communautés californiennes qui, tout au long des années 1990, ont imaginé et conçu ces dispositifs techniques pour dessiner le cadre d'un nouveau champ de l'interaction économique à l'intérieur du cyberespace. C'est aux imaginaires et aux idéologies de ces mêmes communautés qu'est consacrée cette contribution basée sur l'analyse d'un vaste corpus d'archives de mails de la décennie 1990, la liste de diffusion de la communauté virtuelle des cypherpunks (voir encadré).

Peuplée de hackers, d'activistes et d'ingénieurs, la communauté des *cypherpunks* s'est fixée pour mission le développement et la diffusion de la cryptographie civile en ligne afin d'étendre son usage, jusqu'alors monopolisé par les États et les grandes corporations, aux interactions sociales et économiques des individus dans le cyberespace. Soucieux d'offrir aux individus des moyens de transaction en ligne dotés des mêmes propriétés que l'argent liquide (anonymat, intraçabilité, infalsifiabilité), les *cypherpunks* ont inventé, pour une grande part, les protocoles cryptographiques qui ont contribué à la naissance des cryptomonnaies (Finney, 1993). Les échanges de la liste

offrent d'ailleurs un regard privilégié sur les nombreuses tentatives de création de protocoles d'argent liquide digital qui ont ponctué l'histoire de la communauté. Mais ce sont les échanges et controverses consacrées à la nature et aux enjeux du *digital cash* que nous avons choisi d'analyser ici. Des échanges qui offrent un étonnant panorama des imaginaires et des idéologies qui ont informé le développement des technologies cryptographiques en réseau. Pour comprendre l'importance du concept d'argent liquide digital dans l'entreprise collective des cypherpunks, il est nécessaire de faire un détour par la figure tutélaire du *ecash*, le cryptographe californien David Chaum. Premier à proposer un protocole d'argent liquide digital dans un article de 1985, Chaum y insiste aussi sur la nécessité d'en presser l'actualisation face à l'imminence de la *cashless society*. C'est sur la base de ses travaux et de leurs implications politiques que vont se concentrer une part disproportionnée des échanges de la communauté consacrés au *digital cash* au cours des premières années de son existence (Chaum est cité pas moins de 1113 fois entre 1992 et 1994).

La réception des idées de Chaum s'explique également au prisme des imaginaires foisonnants qui traversent la Baie de San Francisco (ou *Bay area*) des années 1990 où se dessine la fabrique du « Nouveau Monde » digital. L'héritage idéologique de la contre-culture, la cyberculture underground et la hard science-fiction californienne y forment un ensemble à la fois kaléidoscopique et cohérent dont les échanges de la liste de diffusion analysés ici offrent une saisissante matérialité.

Mais ces échanges révèlent aussi la proximité des *cypherpunks* avec l'idéologie néolibérale américaine et plus encore avec les courants extrêmes de l'économie politique libertarienne et anarcho-capitaliste. La sécrétion des idées crypto-anarchistes développées par les *cypherpunks*, qui font l'objet d'innombrables commentaires et controverses sur la liste de diffusion, offre une synthèse qui éclaire ces affinités électives entre les imaginaires de la *Bay area* et les idéologies anti-étatistes américaines. C'est à cette « crypto-anarchie » instrumentée par l'argent liquide digital et autorisée par la structuration d'une économie de marché en réseau que nous nous intéresserons dans un deuxième temps afin d'éclairer les motifs idéologiques qui ont présidé au déploiement des cryptomonnaies.

Loin de se réduire à un programme d'économie politique, les « interactions crypto-médiatisées » dans le cyberespace sont aussi pour les *cypherpunks* le support imaginaire de techno-utopies sociales articulées autour des principes de décentralisation et d'auto-organisation. Les membres de la communauté virtuelle des extropiens, dont les plus prolifiques contributeurs de la liste *cypherpunk* étaient également des membres actifs, identifieront ces mêmes utopies au territoire privilégié d'actualisation de leurs quêtes technoscientifiques d'immortalité : voyage dans l'espace, transport de capitaux dans le futur, extension radicale de la vie, financement de projets exploratoires aux frontières de l'humain…C'est à ces crypto-utopies que nous

consacrerons la dernière partie de cette exploration dans le futur antérieur des cryptomonnaies.

La liste de diffusion *cypherpunk*

Créée en 1992 et hébergée jusqu'en 1999 sur les serveurs de John Gilmore, la liste de diffusion de mail des *cypherpunks* figure parmi ces « communautés virtuelles » de pionniers (voir Rheingold, 1996) qui ont contribué de manière significative au développement civil de l'internet. Articulée autour d'un noyau dur de hackers californiens, la communauté comptait moins d'une centaine de contributeurs l'année de sa création pour atteindre un peu plus de 700 en 1994 et enregistrait cette même année jusqu'à 40 échanges de mails par jour. Entre 1992 et 1999, les *cypherpunks* ont échangé pas moins de 64 000 messages archivés et accessibles en exhaustivité sur plusieurs sites internet. Ces échanges de mails offrent un matériel ethnographique de première main permettant d'observer, dans leur séquentialité (grâce aux boucles de messages identifiables par leur objet) et dans la temporalité même de leur contexte d'énonciation (les mails étant horodatés), les interactions sociales qui ont animé l'entreprise collective des *cypherpunks*. Si une part importante de ces échanges porte sur des considérations purement techniques, les cypherpunks n'ont cessé de questionner et de co-construire, sous l'égide de leurs fondateurs, le sens de leur entreprise au cours de débats et de controverses heuristiques.

Bien que virtuelle, la communauté des *cypherpunks* reste une « communauté imaginaire et imaginée » (Anderson, 1991) qui s'est construite dans le temps autour de cadres référentiels communs. Certains échanges « rituels » sont particulièrement instructifs à cet égard comme les mails initiatiques destinés à présenter la communauté aux nouveaux entrants (incluant la bibliothèque idéale du parfait *cypherpunk*) ou les états des lieux annuels proposés par les membres fondateurs. La liste offre un accès privilégié au vaste corpus (textes fondateurs, roman cyberpunk, cryptologie, économie politique) à partir duquel s'est élaborée la grammaire d'action propre à la communauté *cypherpunk*. Les relais de mail par communautés virtuelles interposées, les commentaires d'articles de presse, les présentations et les comptes rendus d'innombrables rencontres, conférences et événements qui animent la Silicon Valley des années 1990 permettent aussi de saisir le contexte euphorisant dans lequel évoluent ces artisans du nouveau monde digital.

Dans une démarche exploratoire inspirée de l'interactionnisme symbolique, nous avons fait le choix délibéré de suivre les controverses concentrées sur le déploiement hypothétique du *digital cash* et à partir desquelles s'est élaboré de façon collective le sens de ces innovations présumées. Le volume de données rend cependant la tâche analytique complexe. L'utilisation de logiciels d'exploration de corpus (comme le logiciel *antConc*) nous a permis de repérer rapidement toutes les expressions renvoyant au champ lexical de l'argent liquide digital et d'explorer, grâce aux indices d'indexicalité qui entourent les termes recherchés, les débats les plus pertinents pour notre investigation. Si nous n'utilisons dans cet article que quelques *verbatim* extraits de ces échanges, l'exploration de la liste a cependant guidé toute notre investigation afin de mettre en lumière le « réseau de discours » à partir duquel s'est élaborée l'idée d'argent liquide digital.

Les archives de la liste de diffusion sont accessible sur :
https://mailing-list-archive.cryptoanarchy.wiki/ (consulté le 20/06/22)

LA PRÉHISTOIRE DES CRYPTOMONNAIES

E-cash : le contre-projet de la cashless society

Si la blockchain et les cryptomonnaies sont le produit d'innombrables briques de développement technologique qui se sont agrégées depuis le milieu des années 1970 dans le champ de la cryptographie (Sherman et al., 2019), leur dessein ne voit réellement le jour qu'au milieu des années 1980 à travers les propositions de David Chaum. Chaum expose l'idée d'un protocole d'argent liquide digital dans un article aux consonances à la fois techniques et politiques dont le titre permet de bien saisir la teneur : « système de transaction pour rendre Big Brother obsolète » (1985). Les communautés virtuelles de hackers qui naissent au début des années 1990 vont non seulement attribuer à Chaum la paternité du *digital cash* mais aussi puiser dans ses écrits le sens politique de leur entreprise.

Pour ce dernier, l'inéluctable émergence d'une informatique en réseau généralisée, et avec elle celle de la *cashless society*, présentait le double danger d'une société faisant de la surveillance des transactions entre agents humains son principal fonds de commerce

en même temps qu'un outil de contrôle et de profilage des populations sans commune mesure. Une prophétie que la massification des usages de l'informatique en réseau au milieu des années 2000 est loin d'avoir démentie. Non seulement les géants du web ont situé la surveillance et le profilage des utilisateurs au cœur de leur modèle d'affaires, tant pour l'optimisation de leur service que celui du placement publicitaire, mais les États-nations, indistinctement autoritaires ou libéraux, n'ont pas manqué d'exploiter les potentialités panoptiques des technologies digitales[1]. Anticipant les dangers inhérents à la digitalisation des communications et des transactions en ligne[2], Chaum sera le premier à proposer un système concret d'argent liquide digital sur internet (1990). Le *e-cash* de la société Digicash, qui ne sera déployé qu'en 1995, en sera la première et brève expérimentation[3].

C'est sous l'impulsion de ses travaux que va se cristalliser en 1992 la communauté virtuelle des *cypherpunks* initiée par des hackers et des ingénieurs issus pour la plupart des entreprises pionnières de la baie de San Francisco (Intel, Netscape, Sun Microsystem, Apple, AMIX, Xanadu, Xerox…) autour de ce qui pourrait s'assimiler à une véritable croisade libertaire destinée à déjouer les plans de la « société de contrôle ». La *cashless society*, écrira l'un de ses fondateurs, constitue « la plus grande des menaces à laquelle notre liberté et notre futur sont confrontés ».

> Si le gouvernement parvient à créer cette cashless society, il disposera alors d'un pouvoir sans précédent sur tous les aspects de nos vies. Toutes les transactions, aussi triviales soient-elles, seront enregistrées, stockées et soumises à analyse. Il existera alors un audit complet des poursuites d'achats, des préférences alimentaires, des choix de divertissements, de liens sociaux… Nous devons élaborer dès maintenant un plan pour l'éviter. (De : Timothy C. May. À : extropians@gnu.ai.mit.edu. Objet : Scenario for a Ban on Cash Transactions. 24/11/92)

Mues par des postures conspirationnistes[4] et libertariennes héritées de la contre-culture de la fin des années 1960, les *cypherpunks* font partie de ces communautés virtuelles de pionniers qui ont significativement contribué à l'évolution d'internet en s'attachant à produire des agencements techniques fidèles à leur

[1] On pense évidemment aux révélations du lanceur d'alerte Edward Snowden, à l'affaire Cambridge Analytica ou encore à la mainmise du gouvernement chinois sur les données des géants du numérique asiatiques.

[2] À une époque où se déploient massivement les cartes de débit électroniques et où la guerre contre la drogue initiée par l'administration Nixon a doté le FBI et les services de renseignements américains de moyens colossaux en matière de surveillance, avec en arrière-plan le Watergate ou le programme de surveillance COINTELPRO qui ont profondément attisé la méfiance à l'égard de l'État et des grandes corporations.

[3] Faute d'utilisateurs, la société Digicash cessera ses activités à la fin des années 1990. Le système mis en place par Chaum, en plus d'être breveté (le rendant de facto impossible à développer par des communautés de hackers), ne pouvait fonctionner qu'avec le concours des banques et n'était, pour cette même raison, que partiellement anonyme.

[4] Le déploiement des cartes de débit électroniques sera notamment associé dans la cyberculture underground californienne à des imaginaires conspirationnistes aux accents apocalyptiques, elles figureraient la « marque de la bête » métaphoriquement imagée par des codes-barres tatoués sur la nuque des individus. Voir par exemple Real (1991)

projection imaginaire. C'est à ces imaginaires « techno-futuristes » qu'il faut s'intéresser pour comprendre la genèse de ces dispositifs d'un genre nouveau.

Communautés virtuelles techno-futuristes

L'internet est un étonnant lieu de paradoxe : massivement financé par l'État et le complexe militaro-industriel, développé par des libertariens marqués par l'éthos de la contre-culture et mis sur le marché par des industriels néolibéraux aux penchants anarchistes (Barbrook et Cameron, 1996). Toujours est-il que la position oscillante occupée par ces communautés de pionniers, à l'interstice des financements de l'État, du développement civil de l'informatique en réseau et de sa mise en marché, a dessiné la toile de fond sur laquelle s'est déployé le développement technologique de l'informatique en réseau (Turner, 2008).

La communauté virtuelle des *cypherpunks* incarne à merveille ces ambivalences. Ses trois fondateurs (voir illustration 1), Timothy May, Eric Hughes et John Gilmore étaient de brillants scientifiques d'une trentaine d'années issus des grandes universités californiennes et engagés dans les entreprises pionnières de la Silicon Valley. Timothy May, physicien de formation embauché chez Intel, prendra une retraite anticipée à l'âge de 34 ans à la suite de sa découverte relative aux effets des particules alpha sur la production des microprocesseurs. Cofondateur avec John Perry Barlow de l'Electronic Frontier Foundation, John Gilmore était le cinquième employé de l'entreprise Sun Microsystem, dont il se retirera lui aussi très tôt après avoir accumulé suffisamment de capital pour subvenir à ses besoins jusqu'au restant de ses jours (Brunton, 2020). Brillant mathématicien diplômé de l'université de Berkeley, Eric Hugues participa de son côté à la brève aventure de la société digicash de David Chaum et poursuit aujourd'hui encore une (très) discrète carrière d'ingénieur en cryptographie.

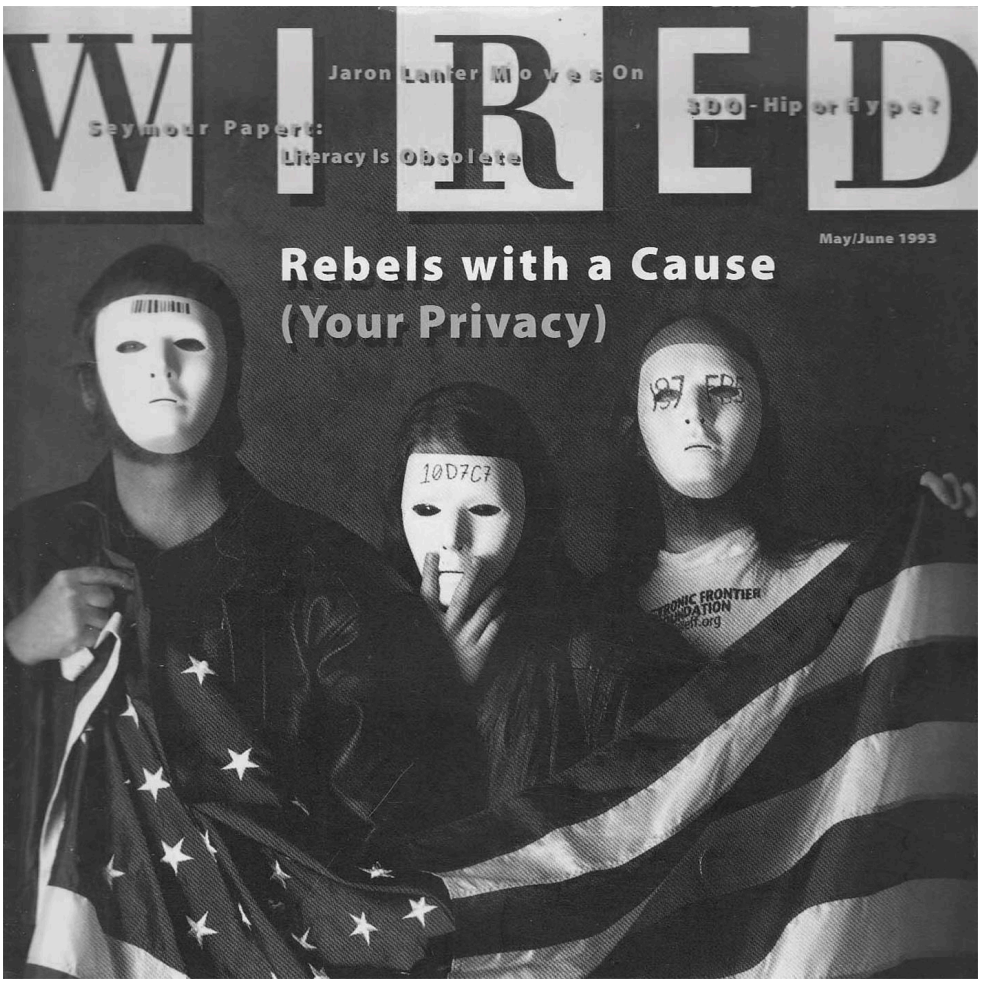

Illustration 1 : Rebel with a cause (your privacy)
Source : première de couverture de *Wired*, mai/juin 1993
De gauche à droite Timothy May, Eric Hughes et John Gilmore dissimulant leur identité civile derrière un masque sur lequel on peut voir leur clef publique (leur identité cryptographique). Bien qu'en apparence contradictoire, la présence du drapeau américain renvoie ici aux valeurs individualistes et libérales de la nouvelle nation et à une certaine culture de la désobéissance civile.

Si l'essentiel des échanges de la communauté se fait via la liste de diffusion de mail, les *cypherpunks* de la baie de San Francisco se réunissent régulièrement dans des meetings physiques organisés dans les bureaux de John Gilmore. Ces rencontres, qui font l'objet de comptes rendus détaillés dans la liste de diffusion, invitent également des hackers et ingénieurs d'autres communautés de la *Bay area* à partager leur réalisation dans le contexte euphorisant de la fabrique du Nouveau Monde digital. Elles sont aussi l'occasion d'expérimenter à partir de la théorie des jeux, des jeux de rôles (le *crypto-anarchist game*) qui engagent des problématiques cryptographiques. Des « situations » à partir desquelles les cypherpunks imaginent collectivement les solutions techniques à mettre en œuvre pour concevoir leurs protocoles cryptographiques.

Un nombre considérable des contributeurs de la liste *cypherpunk* parmi les plus prolifiques était par ailleurs engagé au sein d'une autre communauté virtuelle, celle des extropiens, qui lance sa liste de diffusion un an à peine avant celle des cryptographes californiens. Autoproclamée transhumaniste, la communauté des extropiens balaie un spectre bien plus large de problématiques futuristes que les *cypherpunks* : extension radicale de la vie, cryonie, téléchargement de la conscience (*mind upload*), colonisation spatiale, nanotechnologies… Elle partage en revanche avec elle une même aversion pour le pouvoir étatique, la planification économique et toutes les formes d'organisation bureaucratique qui tendent à brider les potentialités individuelles. L'argent liquide digital figure parmi les centres d'intérêt partagés par ces deux communautés qui interagissent fréquemment par le biais de mails relayés d'une liste de diffusion à l'autre.

Pour comprendre la communauté des *cypherpunks*, il faut encore l'inscrire dans un plus vaste mouvement propre à la Californie de la fin des années 1980 : celui des *cyberpunks*, genre littéraire science-fictionnel qui en est progressivement venu à caractériser la cyberculture underground de la *Bay area*[5]. Sorte de figure hybride entre le hippie marqué par l'éthos de la contre-culture californienne et le bricoleur-technophile baigné dans l'anticipation science-fictionnelle (et le plus souvent ingénieur de formation), les *cyberpunks* se définissent comme des « techno-futuristes libertariens » (Jude et al., 1995). Ces communautés se caractérisent par une méfiance viscérale à l'égard de l'État et de toute autorité centralisatrice. À l'image du leitmotiv hacker, « mistrust authority, promote decentralization » (Rucker, R. et al., 1992), elles prônent les valeurs de la liberté individuelle, de la créativité, du « *Do It Yourself* » et de l'auto-organisation articulées autour de la sacro-sainte notion de réseau. Des postures qui vont également puiser dans le New Age des motifs spirituels (Pucheu, 2021) à l'instar de la revue underground du New Edge (*Edge* pour technologie de pointe) et de la cyberculture de la fin des années 1980, Mondo 2000. C'est d'ailleurs la coéditrice de cette même revue, Judith Milhon alors en couple avec Eric Hughes qui va baptiser le groupe *cypherpunk* : contraction de *cypher* (code secret) et *cyberpunk* (De : Judith Milhon. À : rusirius@well.sf.ca.us. Objet : HOW TO MUTATE AND TAKE OVER THE WORLD. 21/06/94).

La fabrique du futur

Référence omniprésente de la communauté des cypherpunks, la science-fiction d'anticipation de la Californie des années 1980-1990 semble littéralement concourir au Nouveau Monde numérique qui s'y fabrique tant elle interroge en profondeur et

[5] Le Time consacrera notamment sa Une de février 1993 à cette « sous-culture underground futuriste » des cyberpunks californiens. Le Real cyberpunk Fakebook publié en 1995 par les éditeurs de la revue Mondo 2000 (qui met en scène Eric Hughes en couverture) en propose également une synthèse éclairante (Jude et al., 1995).

souvent de façon experte les virtualités des technologies digitales. Les revues et magazines qui innervent la cyberculture californienne de l'époque participent également de cette confusion des genres tant les frontières entre science fiction et ingénierie y semblent souvent indiscernables (Judes et al., 1995).

Outre la perspective d'une mise en réseau généralisée de l'informatique personnelle à la fin des années 1980, l'importance de l'anticipation science-fictionnelle s'explique en grande partie par les perspectives ouvertes par la loi de Moore[6]. Attestée empiriquement depuis la fin 1960, cette loi qui postule l'accroissement exponentiel de la puissance computationnelle (appelée à doubler tous les 18 mois) a d'une certaine manière plongé les ingénieurs informatiques dans une entreprise productive toujours projetée au-delà d'elle-même. La loi de Moore a dessiné une sorte d'espace liminal entre présent et futur, actualité et potentialité du digital qui est devenu le champ imaginaire privilégié de la cyberfiction américaine. Le contexte technologique bouillonnant du début des années 1990 se prêtera particulièrement à ces transactions entre ingénierie et imaginaire science-fictionnel.

L'écrivain et ingénieur en informatique Vernor Vinge en fournit une très concrète illustration. Les fictions futuristes qu'il dépeint dans ses oeuvres, basées sur une connaissance extrêmement précise des technologies numériques, ont pu fournir, du propre aveu de nombreux ingénieurs[7], une orientation décisive à leur entreprise technologique. La très influente nouvelle *True Names* (2001 [1981]) est par exemple la première à mettre en scène une représentation spatiale de l'internet pensé comme monde virtuel (*The Other Plan*). Elle dépeint pour la première fois l'expérience d'individus, dissociés à la fois de leur corps et de leur identité civile (de leurs « *true names* »), interagissant à travers des avatars dans la topographie démiurgique de la réalité virtuelle. Référence récurrente dans la liste de diffusion, l'expression « *true name* » en est venue à qualifier, dans la vulgate des *cypherpunks*, l'identité civile (*off line*) des individus par opposition à leur crypto-identité en ligne : leur pseudonyme, plus communément qualifié de « nym ».

Le cyberpunk de William Gibson, Bruce Sterling ou encore Neil Stephenson, qui font partie des lectures systématiquement recommandées aux nouveaux entrants de la liste *cypherpunk*, offrent des projections futuristes plus centrées sur les conséquences sociopolitiques du déploiement technologique. Bien moins versés dans la fantaisie que l'œuvre de Vinge mais tout aussi informés sur le plan technique, ces auteurs mettent

[6] La loi de Moore formulée en 1965 par le fondateur d'Intel (Gordon Moore) désigne l'accroissement exponentiel de la puissance de calcul, du stockage des données, de la miniaturisation des composants et de la baisse concomitante des coûts de production.

[7] Voir la très instructive réédition augmentée de True Names publiée en 2001 qui propose des contributions d'ingénieurs (dont Timothy May) expliquant l'implication de l'oeuvre de Vinge dans leur propre travail (Vinge, 2001).

en scène un futur proche aux allures dystopiques où règne le plus souvent une forme d'anarchie dans un paysage saturé de technologies. *Snow Crash* (le *Samouraï Virtuel* en français) de Stephenson ou encore *Island of the Net* de Sterling réinventent par exemple des versions techno-futuristes du communalisme utopique dans des espaces virtuels décentralisés. Ces nouvelles offrent, selon l'expression de Timothy May un « regard méchamment satirique (*wickedly satirical*) sur le possible futur proche de l'Amérique » (De : Adam Shostack. À : Timothy C. May. Objet : Crypto's Role in Evil? 09/09/95).

On doit encore à Vinge la notion de « singularité technologique » (1993) qui a contribué à inscrire la loi de Moore dans un horizon d'attente eschatologique (celui d'un dépassement de l'intelligence humaine par la machine) et qui deviendra un élément central de l'imaginaire transhumaniste californien (Pucheu, 2018). Pour les cypherpunks, l'imminence de cette même singularité insufflait à leur entreprise technique un sentiment mêlé d'urgence et d'exaltation. Nous sommes au seuil de la tant attendue « crypto-singularité », écrit Tim May dans un message de 1992.

> Une singularité dans le sens d'une évolution extrêmement rapide dans le champ de la technologie, de la culture [...] Une notion déjà appropriée par les enthousiastes des nanotechnologies pour servir leur propre propos » (De : Timothy C. May. À : cypherpunks@toad.com. Objet : The Crypto Singularity. 12/11/92).

Dans le long inventaire de faits et des événements présageant cette « crypto-singularité », la diffusion grand public du premier logiciel de messagerie électronique permettant d'échanger anonymement des messages chiffrés tout en garantissant l'authentification numérique de ses interlocuteurs, PGP (*Pretty Good Privacy*), occupe une place particulière. Développé par l'ingénieur libertarien Paul Zimmerman et diffusé sous licence libre quelques mois à peine avant la création de la liste de diffusion cypherpunk, PGP a en effet doté pour la première fois des civils d'outils jusqu'alors monopolisés par les services de renseignements et le complexe militaro industriel (Aitken, 1992, p. 12). Pour les *cypherpunks*, le déploiement de PGP basé sur la cryptographie à clef publique marque une étape pivot. « Le génie est presque sorti de la lampe » écrit Timothy May en 1992 et rien, dès lors, ne semble pouvoir empêcher le déploiement de la cryptographie civile en ligne.

> Nous sommes au commencement de quelque chose d'énorme. Alors que je reste sceptique sur les prétentions disruptives de choses comme les nanotechnologies, je considère tout cet ensemble (ball of wax) transnational / cyberespace / cryptologie / monnaie digitale bien_plus_simple à implémenter. Les réseaux se multiplient bien au-delà de toutes les attentes de nos gouvernements, l'accroissement des bandes passantes, des CPUs sont en train de doter les utilisateurs d'incroyables pouvoirs sur leur bureau, PGP génère un intérêt incroyable et les tendances sociales sonnent le temps de la crypto-anarchie (De : Timothy C. May. Objet : Some (Pseudo)Random Thought. 14/09/92).

L'ARGENT CONTRE L'ÉTAT

Épiphanie : Blacknet

David Chaum comme Paul Zimmerman, qui ne participeront que très indirectement à l'aventure *cypherpunk* (seul Zimmerman fut brièvement abonné à la liste), souhaitaient avant tout doter les individus de moyens concrets permettant de protéger leur vie privée face à l'imminence de la société de surveillance. Les cypherpunks vont aller plus loin et faire du déploiement des outils cryptographiques en ligne, à commencer par l'argent liquide digital, le héraut d'une nouvelle ère, celle de la « crypto-anarchie ». Timothy May qui en sera incontestablement le théoricien le plus enthousiaste, expliquait dans un message la genèse de ces idées (De : Timothy C. May. À : cypherpunks@toad.com. Objet : Blacknet worries. 20/02/94).

C'est en évaluant le modèle d'affaires d'un projet de start-up au cours de l'année 1987 que s'est révélée à lui la téléologie politique des technologies cryptographiques. American Information Exchange (AMIX), la start-up en question, qui ne sera réellement active qu'en 1990, était dirigée par l'un de ses amis, Phil Salin (1950-1991), par ailleurs entrepreneur dans l'une des première sociétés privées d'aérospatiale (*Star Trucks*). Économiste de formation fasciné par les mécanismes de marché dépeints par le penseur ultralibéral de l'école autrichienne Friedrich Hayek, Phil Salin était également un futuriste engagé dans le mouvement extropien. Plusieurs ingénieurs de renom et transhumanistes notoires, dont Mark S. Miller (alors ingénieur en chef chez Xanadu) et Eric Drexler (père des nanotechnologies), qui deviendront des amis proches de May, étaient également engagés dans le développement de ce qui peut être considéré comme le premier marketplace de l'internet avant même que n'existe le web.

Centré sur l'échange d'information stratégique, le logiciel AMIX est la première plateforme d'intermédiation mettant librement en relation des vendeurs et des acheteurs, des producteurs et des consommateurs et dont l'activité centrale consistait à orchestrer leurs interactions à la fois financières et sociales grâce à un système de paiement intégré et de contrats personnalisables, les ancêtres des *smart contracts* qui inspireront Nick Szabo (Miller, 1998). Grâce à la baisse des coûts de transaction et aux effets de réseau (le « *fax effect* ») inhérents à la network economy, AMIX pensait de son côté générer une économie substantielle à partir des seules commissions ponctionnées sur les transactions[8]. La plateforme offrait l'architecture d'un libre-marché décentralisé permettant de coordonner les agents économiques à partir des seuls mécanismes de l'offre et de la demande. Elle favorisait ainsi l'émergence dynamique de marchés qui,

[8] Dans les faits, AMIX sera un échec commercial faute de pouvoir bénéficier d'une masse critique d'utilisateurs rendant justement viable un modèle économique basé sur les effets de réseaux (à une époque où le web n'existait pas et où à peine 1 % de la population américaine bénéficiait d'une connexion internet).

indépendamment de toute planification centralisée, laissaient aux seuls agents économiques le soin de déterminer la nature et la valeur des produits qu'ils échangent, fidèle en ce sens à l'idée d'ordres spontanés des marchés (la catallaxie) défendue par Hayek et tout un pan de l'école autrichienne (Bourdeau, 2014).

Ces confluences entre les agencements techniques et les agencements marchands proposés par les économistes de l'école autrichienne ne sont pas fortuites. Comme en témoignera en 1989 un projet informel de recherche mené au sein du think tank néolibéral du *Center for the Study of Market Processes* de la très influente George Mason University (GMU). Le projet *Agoric*, piloté par des économistes de la GMU et auxquels s'associèrent Phil Salin, Eric Drexler, Mark Miller et plusieurs membres actifs de la liste *cypherpunk*[9], avait précisément pour vocation de faire dialoguer les théories du libre-marché de l'école autrichienne avec les *computer sciences*. De façon révélatrice, l'économiste Don Lavoie qui pilotait le projet baptisera ce groupe interdisciplinaire de chercheurs et ingénieurs les « *High Tech hayekians* » (Lavoie, 2004).

À bien des égards, le modèle de l'économie de marché inoculé dans le projet AMIX préfigurait le capitalisme de plateforme qui nous est contemporain. Mais pour May, une place de marché comme AMIX associée à un système d'argent liquide digital, augurait un tout autre avenir : l'émergence d'un marché noir global décentralisé, déterritorialisé et définitivement libéré du joug de la régulation étatique, le « *Blacknet* ».

> J'ai cité à Phil la perspective d'un « BlackNet » (oui, je l'ai nommé ainsi en 1987) qui permettrait d'acheter et de vendre des secrets d'entreprise (et militaires) par le biais de pseudonymes numériques et de mixes [technique rendant les échanges de messages intraçables] à la Chaum. C'est ce à quoi le *Brave New World* allait ressembler. Et c'est ainsi que sont nées les idées cypherpunks (De : Timothy C. May. À : cypherpunks@toad.com. Objet : Laws, Politics, and Crypto Anarchy. 28/12/94).

Le *Blacknet* de Timothy May, qui est loin de se limiter au seul commerce de secrets d'entreprises, n'est pas à proprement parler un projet, il s'agit plutôt d'une vue de l'esprit, d'une sorte d'idéal type figurant ce que pourrait être le futur d'un monde où seraient massivement déployées les technologies cryptographiques. Il offre l'image d'un libre-marché globalisé qui pourrait à terme miner le rôle des gouvernements, voire concourir à leur effondrement. C'est précisément sur le modèle du *Blacknet* qu'émergeront des plateformes articulées sur des protocoles cryptographiques comme *Silk Road*[10], sorte d'Amazon de la drogue qui va populariser pour la première fois l'usage du Bitcoin en 2010 ou encore *Wikileaks*, dont le fondateur, Julian Assange, figurait parmi les membres actifs de la communauté cyberpunk dès l'année 1995.

---

[9] Un message instructif de Timothy May, présentant à l'ensemble de la communauté cypherpunk les connexions qui relient ses membres à ceux de « l'équipe des marchés » de la GMU, révèle les affinités qu'entretient l'entreprise cypherpunk avec les théories du libre-marché défendues par les économistes de l'école autrichienne.

[10] Le fondateur de Silk Road, Ross Ulbritch, aujourd'hui condamné à la réclusion à perpétuité, s'est d'ailleurs explicitement inspiré du Blacknet de May tout en affichant ses affinités avec les théories libertariennes du chef de file de l'école autrichienne, Ludwig Von Mises (Bearman, 2015).

Crypto-anarchie en réseau

« Un spectre hante le monde moderne, le spectre du crypto-anarchisme », écrit Timothy May en préambule du manifeste crypto-anarchiste qu'il rédige en 1988, un an après avoir imaginé le *Blacknet* (May, 2003). Distribué informellement lors des conférences *crypto 88* et *Hacker conference* (1989) de la *Bay area*, ce manifeste peut être lu comme une « utopie de projet » (Flichy, 2001) qui a posé les grandes orientations programmatiques de l'entreprise *cypherpunk*. Le terme crypto-anarchie, écriront plus tard May et Hughes (1992), est un jeu de mots destiné à caractériser, outre l'utilisation d'outils cryptographiques, la nature opaque (« cachée ») d'une forme d'anarchie inhérente au déploiement de l'informatique en réseau (De : Timothy C. May. À : cypherpunks@toad.com. Objet : Crypto Glossary. 22/11/92).

> Le Net est une anarchie. Ce truisme est au cœur de la crypto-anarchie – pas de contrôle centralisé, pas de législateur, pas de leader (sauf par l'exemple ou la réputation), pas de lois. Aucune nation ne contrôle le net, aucune organisation administrative ne détermine sa politique (May, 2001).

Si l'anarchie à laquelle fait référence Timothy May désigne l'approfondissement d'une philosophie politique libertarienne, elle-même héritière d'une longue tradition américaine (celle de l'anarchisme individualiste[11]), elle renvoie avant tout à un courant radical de l'économie politique : l'anarcho-capitalisme. La crypto-anarchie, écrit May, est « la réalisation cyberspatiale de l'anarcho-capitalisme, transcendant les frontières nationales et permettant aux individus de conclure de manière consensuelle l'accord économique qu'ils souhaitent conclure » (2003 [1988]).

Défendu par les émules radicaux de l'école autrichienne d'économie comme Murray Rothbard et plus proche de nous David Friedman (fils du célèbre économiste néolibéral Milton Friedman), l'anarcho-capitalisme procède d'un rejet absolu de l'État, réduit à son plus simple appareil coercitif, en y opposant le droit naturel des individus à disposer librement de leur propriété. Comme l'affirmait Rothbard :

> Le seul moyen « naturel » pour l'homme de survivre et d'atteindre la prospérité consiste à utiliser son esprit et son énergie pour se lancer dans le processus de production et d'échange. [...] Le cheminement de la société dicté par les exigences de la nature de l'homme est donc celui des droits de propriété et du libre-marché du don ou de l'échange de ces mêmes droits (2000 [1974]).

L'État au contraire, reprend Rothbard, « fournit un canal légal ordonné et systématique à la prédation de la propriété privée ; il rend certain et relativement paisible le mode de vie de la caste parasitaire de la société » (*ibid.*). Comme pouvait l'écrire un contributeur de la liste en s'appuyant sur le référentiel libéral de la communauté *cypherpunk* :

> Sans la capacité de contrôler sa propre propriété, tous les autres droits tombent à l'eau. Je suggère de lire *La richesse des nations* d'Adam Smith pour une meilleure compréhension du capitalisme, qui explique pourquoi il s'agit du « seul » modèle

[11] L'historien et politologue Henri Arvo offre une excellente perspective sur cette tradition de l'anarchisme individualiste qui traverse toute l'histoire américaine (1983).

> économique viable pour une société libre. Encore mieux, *La route de la servitude* de F. A. Hayek, qui sape intégralement les bases de l'économie planifiée et montre comment la dépossession de la propriété privée et de la liberté économique par l'État mène directement et inévitablement au totalitarisme (De : Steve Schea. À : William H. Geiger. Objet: Nature of Anarchy /Anarchy of Nature. 19/05/97).

L'État serait d'une certaine façon irrésistiblement mû par l'exercice d'une violence légale visant à déposséder les individus de leur propriété privée au profit de l'accroissement indéfini de sa propre machinerie (Hayek, 2003 [1944]). Le terme « propriété privée », lui-même naturalisé, doit être entendu ici de façon extensive. Il s'étend en effet à toutes les propriétés de l'individu, à son corps, à son comportement, à ce que lui dicte sa conscience, à sa vie même dont lui seul est libre de choisir le cours dans le strict respect de la propriété d'autrui. Le libre-marché n'est donc qu'un autre mot pour désigner le processus par lequel s'exerce l'action libre et souveraine des individus, éclairée par la « praxéologie » (Mises, 1985 [1949]), dans leur rapport au monde (matériel, social, cognitif…). Rapport au monde toujours pensé comme interaction volontaire et consciente orientée vers des finalités propres aux valeurs et intérêts défendus par ces mêmes individus. La concurrence des intérêts individuels, érigée en norme des rapports sociaux, s'affiche ainsi comme l'opérateur privilégié de l'évolution sociale. Une évolution jusqu'alors entravée par les logiques redistributives de l'État et de la prétendue justice sociale qui cacherait les véritables intentions du conservatisme institutionnel. Comme l'illustrent les propos d'Adam Back (inventeur du système de preuve de travail Hashcash) dans un échange controversé autour de la justice sociale.

> Ce qui est insupportable, c'est la « charité » (la sécurité sociale) à la pointe du fusil. Notre « conscience » est dictée par le gouvernement qui agit comme un courtier pour ceux qui font pression pour leurs « besoins » et pour que vos actifs vous soient volés et leur soient redistribués. Ce que les gens ne sont pas prêts à payer ne devrait pas leur être extorqué. [...] Aucun État ne peut gouverner ceux qui ne veulent pas être gouvernés. Oui, mais l'État peut tuer ceux qui ne veulent pas être gouvernés. Il le peut et il le fait fréquemment. C'est ce qui est si fascinant avec le cyberespace, une fois les systèmes de paiement digital en place, les escrocs du gouvernement ne pourront plus exercer leur violence (De : Adam Back. À : cypherpunks@toad.com. Objet: How to solve the tax problem w/o anarchy or force. 10/11/98).

C'est cette même abolition de la violence étatique autorisée par la cryptographie qui présidait aux motivations d'un des projets les plus aboutis d'argent liquide digital proposé sur la liste *cypherpunk*. En préambule de la présentation de son protocole *b-money* publié en 1998 sur la liste (qui préfigurait à bien des égards ce qu'allait être le bitcoin), le cryptographe américain Wei Dei expliquait :

> Je suis fasciné par la crypto-anarchie de Tim May. Contrairement aux communautés traditionnellement associées au mot « anarchie », dans la crypto-anarchie, le gouvernement n'est pas temporairement détruit mais définitivement aboli et définitivement inutile (irrelevant). C'est une communauté où la menace de violence est impuissante parce que la violence est impossible, et la violence est impossible parce que ses participants ne peuvent pas être liés à leurs vrais noms (*true names*) ou lieux physiques (Dei, 1998).

Pour renouer avec cet évolutionnisme de marché défendu par l'anarcho-capitalisme (Ege, 1992) qui radicalise les visions naturalistes du capitalisme d'un Herbert Spencer (irréductiblement associé au darwinisme social qui le caractérise), les *cyberpunks* opposeront à l'action politique l'effectivité des technologies cryptographiques. Il n'a jamais existé, écrivait encore Wei Dei,

> De gouvernement qui n'essaie tôt ou tard de réduire la liberté de ses sujets et d'accroître son contrôle sur eux, et il n'y en aura probablement jamais. Au lieu d'essayer de convaincre notre gouvernement actuel de ne pas essayer, nous développerons les technologies (*remailer* et *ecash*) qui rendront impossible le succès d'une telle entreprise (De : Wei Dei. To : cypherpunks@toad.com. Objet : Law vs technology. 10/02/95).

Débat récurrent sur la liste *cypherpunk*, les échanges autour de l'action politique finissent invariablement par aboutir au solutionnisme technologique à l'image de cette réponse de May adressée à des militants politiques de la protection de la vie privée :

> Je préfère les solutions technologiques aux solutions politiques. N'appelez pas ça de la sédition, mais plutôt la tendance naturelle des technologies. [...] Je pense qu'éduquer le public est une cause perdue. Nous n'obtiendrons jamais la crypto-liberté par les urnes, nous ne l'obtiendrons que si la technologie est solide et déployée suffisamment largement pour que les tentatives de l'arrêter soient vaines. (De : Timothy C. May. À : cypherpunks@toad.com. Objet : The Futility of General Crypto Education? 23/02/93).

Travestissant ses espoirs en fatalité, cette vision de May reste profondément imbue de déterminisme technologique. L'idée d'un seuil, d'une étape pivot à partir de laquelle plus rien ne pourrait empêcher qu'advienne la crypto-anarchie, on le voit ici, doit beaucoup aux perspectives évolutionnistes informées par la loi de Moore et son pendant science-fictionnel (la singularité technologique). Ce qu'il adviendra au-delà de ce seuil est d'une certaine manière déjà écrit pour les hackers californiens dans les scénarios dépeints par les utopies cyberpunks : décentralisation, auto-organisation, anarchie, capitalisme sauvage (Kelly, 1992).

CRYPTO-UTOPIE

Interactions crypto-médiatisées

Les différentes formes de cryptographie forte (*strong cryptography*), écrivait Timothy May dans la foire aux questions de la liste *cypherpunk*,

> contribueront à diminuer le pouvoir de l'État et peut-être même à précipiter son effondrement. Nous pensons que l'expansion dans le cyberespace des communications sécurisées, de l'argent liquide digital (digital cash), de l'anonymité et de la pseudonymité et autres interactions médiatisées par la cryptographie (*crypto-mediated interactions*), changeront profondément la nature des interactions sociales et économiques. Les gouvernements auront de plus en plus de mal à collecter les taxes, à réguler le comportement des individus et des organisations, et plus

> généralement à contraindre les individus alors même qu'ils ne pourront plus savoir de quel continent ils proviennent (May, 1994).

Les pseudonymes sont pour les cypherpunks la pierre angulaire de ce changement de nature des interactions sociales et économiques. Loin de se réduire au simple anonymat, l'usage de pseudonymes numériques revient à doter un individu ou un groupe d'individus d'une identité cryptographique unique (une clef publique) authentifiée numériquement (infalsifiable et inviolable). La création d'un pseudonyme fait d'une certaine manière naître une entité persistante dans l'internet au même titre que la déclaration d'identité civile fait naître un citoyen dans l'espace territorial d'un État (persistant lui aussi jusqu'à sa mort). L'identification civile est précisément le canal privilégié par lequel les États exercent sur les individus la violence légitime dont ils sont dépositaires : emprisonnement, taxation, fiscalité, censure, oppression, expropriation… Usant de pseudonymes dissociés de leur identité civile, les individus pourraient librement établir des contrats, opérer des transactions, dévoiler des secrets, tenir des propos séditieux ou faire acte de désobéissance civile sans craindre l'ingérence d'une quelconque forme d'autorité. Plus rien ne s'opposerait ainsi aux « interactions volontaires » des individus avec leur environnement, libres de choisir, en fonction de leurs valeurs subjectives et de leurs intérêts propres, avec qui et selon quelle modalité ils désirent échanger ou communiquer.

L'argent liquide digital occupe une place centrale dans ces interactions volontaires. Il s'affiche comme vecteur privilégié de la communication sociale tant les *cypherpunks*, nourris des théories naturalistes de l'école autrichienne, tendent à envisager la société sous le seul prisme du libre-marché (Loveluck, 2015). L'argent digital, réduit à sa plus élémentaire morphologie informationnelle (une séquence de code alphanumérique[12] 12), ne serait plus en substance guère différent du discours ou des opinions sur lesquels se fondent les liens sociaux.

> Oui la parole est impliquée. « Argent liquide digital = discours ». Dépenser de l'argent est une façon de communiquer des ordres à d'autres, de transférer des fonds, de débloquer des fonds, etc. En fait, la plupart des instruments financiers ne sont que des contrats ou des ordres et non des entités physiques ou des billets de banque. [...] Restreindre l'usage de l'argent liquide digital irait à l'encontre de la liberté d'expression, puisqu'il sera impossible de savoir, sans le lire préalablement, si un message est un « discours pur » ou s'il présente des aspects caractéristiques de l'argent digital (May, 2003, p. 61).

Cette identification de l'argent liquide digital à une forme de discours n'est pas anodine. Au même titre que le code informatique, envisagé par les cyberpunks comme une forme d'expression protégée par le premier amendement de la constitution américaine (Salin, 1991), l'argent liquide digital, libéré de son support d'inscription matériel, ne serait plus qu'un message dont le contenu relèverait désormais exclusivement de la sphère privée. C'est d'ailleurs cette métamorphose

[12] « L'information est de l'argent. L'information est liquide, traverse les frontières, et est généralement convertible en monnaie réelle », écrit Timothy May dans un message adressé à la communauté cypherpunks en 1992 (10/09/92).

informationnelle de l'argent qui pourrait mettre un terme au monopole exercé par les États et les banques centrales dans l'émission de la monnaie. La fin des politiques inflationnistes permises par ce même monopole, systématiquement associées par les *cypherpunks* à l'exercice d'une violence légale (Golumbia, 2016) ou à une forme de planification économique grossière et inefficiente du gouvernement, participerait elle aussi de ce renversement des rapports de force entre les États et les individus.

Il faut encore rappeler ici que cette confusion entre interaction économique et interaction sociale s'inscrit de façon cohérente dans le montage symbolique américain. Le *Bill of Rights*, que les fondateurs ont rédigé pour protéger constitutionnellement les individus des potentiels abus de l'État, a dessiné les contours d'un espace public structuré sur le modèle d'un marché libre échangiste des idées. Marché à l'intérieur duquel peuvent concourir toutes les opinions, qu'elles émanent d'un individu, d'un groupe d'individu, d'une organisation (séculière ou religieuse) ou même du gouvernement « qui n'est qu'un des participants à ce réseau public de communication et de dissémination de l'information » (Mayali, 2002). L'argent liquide digital, envisagé comme de la « pure » information, ne ferait ainsi que parachever cette logique de libre compétition des opinions inoculée dans l'espace public américain en faisant rentrer les transactions économiques dans le giron de la liberté d'expression individuelle. Un espace public libre-échangiste des opinions et des marchandises à l'intérieur duquel le gouvernement, écrivait Timothy May, désormais « incapables d'exercer le monopole légal de la coercition, ne serait plus qu'un prestataire de service comme Safeway, Goodyear ou K-Mart » (De : Timothy C. May. À : cypherpunks@toad.com. Objet: Voluntary Governments ? 04/08/94).

Mais la disparition des tiers de confiance (l'État et les banques en premier lieu) dans ces transactions économiques volontaires, libérées de toutes entraves légales, laisse en suspens la question de la fiabilité des individus usant d'identité cryptographique.

> Qu'est-ce qui empêchera les gens de renier leur engagement dans le cyberespace ? Pour quelles raisons resteraient-ils honnêtes ? Si le gouvernement et la justice ne peuvent plus traquer un individu qui utilise des systèmes anonymes et intraçables, comment les sociétés et les économies digitales fonctionneront-elles ? (May, 2001).

La solution réside, aux yeux des *cypherpunks*, dans le déploiement de systèmes de réputation anonymes qui guideront le libre choix des individus d'interagir ou non avec une crypto-entité. La réputation exercerait en retour sur leur comportement une sorte d'auto-gouvernementalité les incitant, dans l'optique de maximiser au fil du temps ce même capital réputationnel, à respecter leur engagement et *in fine* à respecter la propriété d'autrui. Mais cette mécanique réputationnelle n'a pas simplement pour vertu d'inciter les *nyms* à respecter la propriété d'autrui. En rendant les comportements et les transactions des *nyms* transparents aux yeux de tous, la réputation fournit l'information nécessaire à la coordination d'individus mus par des intérêts et des valeurs réciproques ouvrant vers des formes de collectifs exclusivement volontaires. Ces mêmes interactions volontaires pourraient, à terme, actualiser les projections

cyberpunk d'un nouveau communalisme dessinant les contours d'une société anarchique à l'intérieur de laquelle pourraient concourir et commercer des communautés disposant de systèmes légaux et de valeurs qui leur sont propres. Sentiment amplifié par l'aventure des communautés virtuelles des années 1990 qui en seraient en quelque sorte le prototype.

> Chaque communauté aura ses propres lois, ses propres politiques d'accès, ses rites initiatiques, ses propres politiques de censures, etc. Les gouvernements auront très peu de pouvoir pour contrôler ces groupes privés, et encore moins lorsque la cryptographie forte offrira une nouvelle topographie pour la connectivité. Des communautés qui seront fondamentalement caractérisées par leur nature essentiellement volontaire (May, 2001).

L'économiste anarcho-capitaliste David Friedman, dont l'ouvrage *The Machinery of Freedom* a constitué, de l'aveu de Timothy May, un référent central dans la sécrétion des idées crypto-anarchistes, ne disait pas autre chose lorsqu'il affirmait :

> Des personnes différentes poursuivent des objectifs différents. Chacun est égoïste uniquement dans ce sens qu'il accepte et suit sa propre perception de la réalité, sa propre vision du bien. Les personnes désireuses de vivre dans une société vertueuse, entourées de personnes partageant leur même conception de la vertu, seraient libres d'établir leurs propres communautés, et de passer des contrats les unes avec les autres pour empêcher les « pêcheurs » d'acheter ou de louer au sein de leurs groupes. Ceux qui souhaiteraient vivre en « communauté » pourraient fonder leurs propres communautés. Mais personne n'aurait le droit d'imposer à son voisin sa manière de vivre (Friedman, 2007 [1973]).

Les *smart contracts*, qui permettent de s'affranchir de toute autorité légale dans la détermination, l'exécution et la validation de contrats scellés entre individus, s'intègrent dans ce même dessein. Au cœur des contrats privés électroniques défendus par Nick Szabo (1996), *cypherpunk* et extropien de la première heure, siège l'idée d'une « production privée de la loi » (*Privately Produced Law*), conceptualisée par le cofondateur du mouvement extropien Tom Bell (Bell, 1991). L'émergence de « systèmes légaux multiples mis en compétition » fournirait l'armature légale au principe d'auto-organisation du projet crypto-anarchiste. Compétition entre communautés qui laisserait libre cours à l'exercice des lois de la sélection naturelle sur les termes de l'évolution sociale.

Expansion illimitée

La communauté virtuelle des extropiens partage avec les cryptographes californiens le même référentiel libertarien et anarcho-capitaliste. Mais le régime anarcho-capitaliste qu'appellent de leurs vœux les extropiens ne constitue pas une fin en soi : il s'affiche comme condition de possibilité de la libération des énergies productives et créatives des individus (concentrée dans le principe extropien de « l'expansion illimitée »). Comme dans la célèbre nouvelle de la philosophe et essayiste libertarienne Ayn Rand *Atlas Shtrugged* (1999 [1957]), les extropiens rêvent d'établir des communautés totalement indépendantes des États où pourraient enfin s'exprimer, dans toutes leurs

latitudes, les potentialités individuelles bridées par la planification étatique[13]. Ils envisagent le libre marché à la lumière de la théorie des ordres spontanés de Hayek (qui figurent aussi parmi les "grands principes" extropiens), comme l'aboutissement d'une sorte d'évolutionnisme cosmique à partir duquel l'humanité pourra franchir une nouvelle et ultime étape, celle de la post-humanité (voir illustration 2).

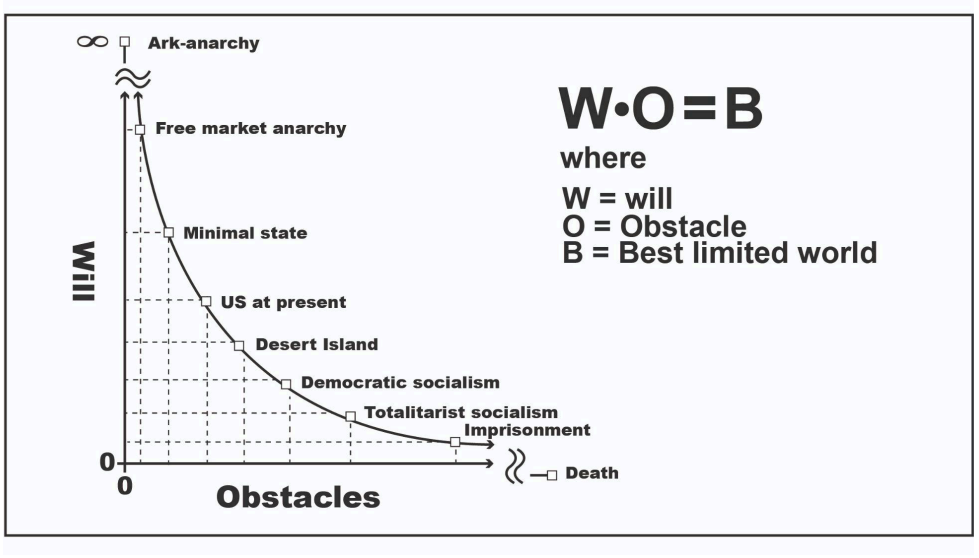

Illustration 2v : *The Ark-anarchist graph of reality*
Source : Reproduction extraite de A. (1990), Ark-anarchy, *Extropy*, n° 5.
Ce graphe présente de façon synthétique les deux polarités cosmologiques entre lesquelles oscille l'Amérique de 1990 : d'un côté l'entropie ou la mort qui résulterait d'une absolutisation du socialisme abolissant les volontés individuelles et de l'autre l'« Arch-anarchie » ou condition post-humaine qui serait au contraire le produit d'un affranchissement progressif vis-à-vis des États au profit d'une liberté individuelle sans borne.

Comme Hayek l'avait suggéré, « l'avantage de la liberté est de laisser le champ libre au futur imprévisible » (1976) et les extropiens, « à l'avant-garde du futur », veulent concourir dès à présent à ce devenir encore imprévisible dans toutes les trajectoires ouvertes par les progrès technoscientifiques. Pour les extropiens, un libre-marché sans autorité ni centre offrirait les conditions de possibilité d'une expansion sans limites du progrès technoscientifique. Il laisserait notamment le champ libre aux travaux d'ingénierie exploratoire (Drexler, 1988) les plus audacieux entravés jusqu'ici par la planification économique et le pouvoir légaliste des États et des grandes corporations.

L'argent liquide digital, actualisant le projet de dénationalisation des monnaies que Friedrich Hayek avait déjà esquissé (More, 1995), offre la possibilité d'établir de

[13] C'est précisément ce que le magnat de la Tech Peter Thiel et le très libertarien petit-fils de Milton Friedman (Patri Friedman) tentent aujourd'hui d'actualiser dans leur projet du Seasteading Institute visant à élaborer des îles artificielles accueillant des pépinières d'entreprises innovantes dans les zones maritimes internationales en marge des États.

nouveaux canaux de circulation du capital en marge des États et des grandes corporations pour financer ces projets d'ingénieries exploratoires souvent à la limite de la légalité (Brunton, 2020). Il offre les conditions d'émergence de marchés totalement autonomes à l'image du *Blacknet* de May qui pourrait favoriser et accélérer les innovations technologiques les plus radicales à l'instar des projets d'extension de la vie qui animent la communauté (pharmacologie anti-âge, clonage thérapeutique, thérapie génique, hybridation homme-machine, cryonie, nanotechnologie…).

Il répond également à une problématique centrale de la cryonie qui concentre l'attention de la communauté dès sa naissance. Procédé de conservation biologique, la cryonie a pour fin d'empêcher la dégradation du corps ou du cerveau d'individus, « fraîchement » cryogénéisés après leur mort, dans l'optique de leur réanimation dès lors qu'une technologie suffisamment avancée le permettra. Qu'elle soit d'ordre biologique (par le truchement des nanotechnologies) ou purement informationnelle (la modélisation computationnelle de notre personnalité), cette seconde et éternelle vie promise par l'innovation technoscientifique aura un coût (Hanson, 1994). Dans un message adressé à la communauté des *cypherpunks*, Timothy May formulait en ces termes les problématiques que les « immoralistes » adressaient à la cryptographie :

> Envoyer de l'argent dans le futur, tout en le préservant de la saisie, de la fiscalité, etc. Cela peut intéresser les personnes cryonisées qui souhaitent organiser leur propre renaissance/réanimation à un moment donné dans le futur. Les systèmes existants reposent sur la création de dotations, de contrats d'assurance, de fonds fiduciaires, etc. La confiance en l'agent est le moyen d'envoyer des fonds dans le futur – il est clair que cet agent pourrait être compromis, perquisitionné, taxé, mis en faillite... Bien que je ne sois pas personnellement un client de la cryonie, j'ai commencé à réfléchir à ce problème en 1989 et j'en ai discuté avec Phil Salin, qui, ironiquement, est maintenant lui-même en suspension cryonique (De : Timothy C. May. À : cypherpunks@toad.com. Objet : Time release crypto. 17/02/93).

L'une des réponses à cette question réside pour Timothy May dans la création d'« institutions persistantes » distribuées qui présageaient d'une certaine manière ce qu'allaient devenir les blockchains.

> Les « institutions persistantes » sont ce que j'appelle ces systèmes ou fiducies qui durent plusieurs décennies. Si de tels systèmes peuvent être construits, en utilisant certaines des idées discutées ici dans ce groupe, alors de nouvelles structures financières et politiques intéressantes sont possibles (De : Timothy C. May. À : cypherpunks@toad.com. Objet : Time release crypto. 17/02/93).

Le cryptographe Hal Finney, décédé en 2014 des suites de la maladie de Charcot et dont le corps est aujourd'hui en suspension cryonique dans les couloirs d'Alcor (la société de cryonie dirigée par les extropiens) pensait sans doute, dans un futur lointain, bénéficier de ces « institutions permanentes » que sont devenues les blockchains. Outre son implication majeure dans la communauté *cypherpunk* et celle des extropiens, Finney fut l'interlocuteur privilégié du mystérieux inventeur du Bitcoin avec qui il opéra la première transaction de cryptomonnaie. Il emporta ainsi dans son « voyage

vers le futur », une somme considérable de bitcoins dont seule sa clef publique pourra, un jour peut-être, lui permettre de revendiquer la propriété…

CONCLUSION

Loin de nous être contemporain, le projet des cryptomonnaies, qui ne s'est effectivement déployé qu'en 2008, se confond avec les utopies technologiques et les imaginaires qui ont accompagné le développement précoce de l'informatique en réseau au cœur de la Californie des années 1990. L'argent liquide digital siège au centre d'un projet de réformation sociale que les pionniers de la cryptographie en réseau appelaient de leurs vœux. Un projet qui partage d'étonnantes affinités électives avec les courants radicaux du libertarianisme américain.

Mais la sacralité de la sphère individuelle dont les crypto-anarchistes se font les hérauts s'inscrit plus largement dans le *Weltgeist* du Nouveau Monde, comme peuvent l'illustrer les idées calvinistes d'une communauté de fidèles réunie en vertu de la seule volonté individuelle de ses membres (*Willinghood*, voir Miall, 1848), l'individualisme protestant approfondi par le transcendantalisme ou encore le proto-anarchisme d'un Thoreau… L'anarchisme individualiste du XIXe siècle (Arvo, 1983), qui prolonge ces imaginaires, figure également parmi les idéologies qui, associées aux prescriptions économiques libertariennes de l'école autrichienne, ont profondément informé le projet de déploiement de l'argent liquide digital. Un individualisme radical également célébré par les extropiens comme le terrain d'accomplissement d'un dessein cosmique promis par la technoscience.

Malgré la naïveté de l'utopie crypto-anarchiste qui laissait envisager un monde où tous les individus s'approprieraient mécaniquement les potentialités disruptives des protocoles cryptographiques (comme l'usage systématique de crypto-identités dans le cyberespace), les *cypherpunks* ont joué un rôle décisif, tant sur le plan technique que symbolique, dans l'émergence des communautés de hackers qui ont bourgeonné sur la planète. Le dark web, les plateformes comme *Silk Road* ou *Wikileaks*, le mouvement contemporain des *Anonymous* sont tous redevables, d'une manière ou d'une autre, aux idées crypto-anarchistes cristallisées par Timothy May et la communauté cypherpunk.

À l'exception des membres de ces communautés, la nature potentiellement anonyme et intraçable des cryptomonnaies n'est pas, loin s'en faut, au centre des motifs de leurs usages contemporains. Usages qui semblent au contraire s'inscrire pleinement dans le capitalisme financiarisé qui caractérise notre système économique tout en en repoussant les limites décentralisatrices. Certes, les communautés contemporaines qui se sont agrégées autour des cryptomonnaies restent marquées pour une bonne part par l'éthos des *cypherpunks*, mais la diffusion grand public du *digital cash*, comme son épanouissement au sein du capitalisme digital, en offrent une vision pour le moins

nuancée (2016). Pour reprendre la célèbre formule de l'École des Mines, « adopter une innovation, c'est l'adapter » et cette adaptation « résulte d'une élaboration collective, fruit d'un intéressement de plus en plus large » (Akrich et al., 1988). Mais si les prétentions disruptives des cryptomonnaies n'ont pas encore rencontré le concours des masses, les scripts d'usages (Akrich, 1987) imaginés par les communautés techno-futuristes californiennes restent, aujourd'hui encore, irréductiblement inscrits dans les agencements techniques qu'elles ont contribué à produire.

RÉFÉRENCES

A (1990), Arch-Anarchy, *Extropy,* n° 5, p. 11-19.
AITKEN D. (1992), Encryption : son of PGP, *Mondo 2000*, n° 9, p. 12-16.
AKRICH M. (1987), Comment décrire les objets techniques ? *Techniques et culture*, n° 9, p. 49-64.
AKRICH M., CALLON M., LATOUR B. (1988), À quoi tient le succès des innovations ? Partie II : Le choix des porte-parole, *Gérer et comprendre*, n° 12, p. 14-29.
ANDERSON B., (1991), *Imagined communities: reflections on the origin and spread of nationalism*, Londres, Verso.
ARVO H. (1983), *Les Libertariens américains : de l'anarchisme individualiste à l'anarcho-capitalisme*, Paris, PUF.
BARBROOK R., CAMERON A. (1996), The Californian ideology, *Science as Culture,* vol. 6, n° 1, p. 44-52.
BIRNER J., GARROUSTE P. (2004), *Markets, Information and Communication: Austrian Perspectives on the Internet Economy*, New-York, Routledge.
BEARMAN J. (2015), The Untold Story of Silk Road, *Wired*, mai.
BECKER K. (2018), La technologie blockchain et la promesse crypto-divine d'en finir avec les tiers, *Études digitales*, n° 6, p. 33-52.
BELL T. (1991), Privately Produced Law, *Extropy #7*, vol. 3, n° 1, p. 12-21.
BOURDEAU M. (2014), L'idée d'ordre spontané ou le monde selon Hayek, *Archives de philosophie*, vol. 77, n° 4, p. 663-687.
BRUNTON F. (2020), *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*, New York, Princeton University Press.
CHAUM D. (1985), Security without identification: transaction systems to make big brother obsolete, *Communications of the ACM*, vol. 28, n° 10, p. 1030-1044.
CHAUM D., FIAT A., NAOR M. (1990), « Untraceable Electronic Cash », in S. GOLDWASSER (ed.), *Advances in Cryptology – CRYPTO' 88. Lecture Notes in Computer Science*, New York, Springer.
DE FILIPPI, P., LOVELUCK B. (2016), The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure, *Internet Policy Review*, Alexander von Humboldt Institute for Internet and Society, vol. 5, n° 3.
EGE R. (1992), Émergence du marché concurrentiel et évolutionnisme chez Hayek, *Revue économique*, vol. 43, n° 6, p. 1007-1036.
DEI W. (1998), *B-money protocol,* novembre. [En ligne] Disponible à l'adresse :

http ://www.weidai.com/bmoney.txt (consulté le 01/04/22).
DREXLER K. E (1988), « Exploring Future Technologies », in J. BROCKMAN (ed.), *The Reality Club*, New York, Lynx Book, p. 129-150.
FINNEY H. (1993), Protecting privacy with electronic cash, *Extropy #10*, vol. 4, n° 2, p. 8-15.
FLICHY P. (2001), La place de l'imaginaire dans l'action technique. Le cas de l'internet, *Réseaux*, vol. 5, n° 109, p. 52-73.
FRIEDMAN D. (2007) [1973], *Machinery of freedom, guide to a radical capitalism*, New York, Routledge.
FRIEDMAN D. (2011), *Future Imperfect: Technology and Freedom in an Uncertain World*, Cambridge, Cambridge University Press.
GOLUMBIA David (2016), *The Politics of Bitcoin. Software as Right-Wing Extremism*, Minneapolis, University of Minnesota Press.
HANSON R. (1994), If upload come first, *Extropy #13*, vol. 6, n° 2, p. 10-16.
HAYEK F.-A. (1976), *Droit, législation et liberté, vol. 1, Le mirage de la justice sociale*, Paris, PUF.
HAYEK F.-A. (2003) [1944], *La route de la servitude*, Paris, PUF.
HUGHES, E. (1992), *The cypherpunk manifesto*, mars. [En ligne] Disponible à l'adresse : https ://www.activism.net/cypherpunk/manifesto.html (consulté le 01/04/22).
JUDE S., SIRIUS R.U., NAGEL B. (1995), *Cyberpunk Handbook: The Real Cyberpunk Fakebook*, New York, Random House.
KELLY K. (1993), Cypherpunks, E-Money and the Technologies of Disconnection, *Whole Earth Review*, n° 79.
LAVOIE D. (2004), « High Tech Hayekians », in J. BIRNER, P. GARROUSTE (eds), *Markets, Information and Communication : Austrian Perspectives on the Internet Economy*, New York, Routledge, p. 91-126.
LOVELUCK B. (2015), Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique, *Réseaux*, vol. 4, n° 192, p. 235-270.
MAY T. (1994), *The Cyphernomicon : cypherpunk FAQ and more*, septembre. [En ligne] Disponible à l'adresse : https://nakamotoinstitute.org/static/docs/cyphernomicon.txt (consulté le 22/03/2022).
MAY T. (2001), « True Nyms and Crypto Anarchy », in V. VINGE, *True Names and the Opening of the Cyberspace Frontier*, New York, Tor Books.
MAY T. (2003), « The crypto anarchist manifest » in P. LULOW (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*, Cambridge, MIT Press, p. 61-65.
MAYALI, L. (2002), *Le façonnage juridique du marché des religions aux États-Unis*, Paris, Mille et une nuits.
MIALL E. (1848), *Ethics of Nonconformity, and Workings of Willinghood*, Londres, Ailot & Jones.
MILLER M. (1998), AMIX as a the first Smart Contracting System. [En ligne] Disponible à l'adresse : http://www.erights.org/smart-contracts/history/ (consulté le 20/05/2005)

MISES L. V. (1985), *L'action humaine. Traité d'économie*, Paris, PUF.
MORE M. (1995), Hayek denationalisation of money, *Extropy*, n° 15, p. 19-28.
PUCHEU D. (2018), Religiosité transhumaniste. Les nouvelles frontières de l'ingénierie exploratoire, *Études digitales*, n° 5, p. 53-70.
PUCHEU D. (2021), « Transhumanisme et religiosités, une généalogie américaine », in D. DOAT, F. DAMOUR (Dir.), *Quand le transhumanisme interroge*, Namur, Presses universitaires de Namur, p. 97-111.
RAND A. (1999) [1957], *Atlas shrugged*, New York, Plume.
REAL S. (1991), 666, *Mondo 2000*, n° 4, p. 16-17.
RHEINGOLD H. (1996), *Les communautés virtuelles*, Paris, Addison Wesley.
ROTHBARD M. (2000) [1974], *Egalitarianism as a revolt against nature and other essays*, Auburn, Ludwig Von Mises Institute.
RUCKER R., SIRIUS R U, MU Q. (1992), *Mondo 2000: A User's Guide to the New Edge : Cyberpunk, Virtual Reality, Wetware, Designer Aphrodisiacs, Artificial Life, Techno-Erotic Paganism, and more*, New York, Perennial.
SALIN P. (1991), Freedom of speech in software, juillet, Palo Alto, [En ligne]. Disponible à l'adresse : http://www.toad.com/freedom.speech.software (consulté le 20/03/22).
SHERMAN A.T., JAVANI F., ZHANG H., GOLASZEWSKI E. (2019), On the origins and variations of blockchain technologies, *IEEE Security & Privacy*, vol. 17, n° 1, p. 72-77.
SZABO N. (1996), Smart contracts, building blocks for digital free markets, *Extropy*, vol. 8, n°1, p. 50-64.
TURNER F. (2008), *From Counterculture to Cyberculture*, *Steward Brand, The Whole Earth Network, and The Rise of Digital Utopianism*, Chicago, UCP.
VINGE V. (1993), *The Coming Technological Singularity: How to Survive in the Post-Human Era*, VISION-21 Symposium, Cleveland, 30-31 mai. [En ligne] Disponible sur : https://edoras.sdsu.edu/~vinge/misc/singularity.html (consulté le 15/03/2023).
VINGE V. (2001), *True Names and the Opening of the Cyberspace Frontier*, New York, Tor Books.