



HAL
open science

Bitcoin : les trois âges d'un objet inclassable (OI)

Assen Slim

► **To cite this version:**

Assen Slim. Bitcoin : les trois âges d'un objet inclassable (OI). Journal des anthropologues, 2022, 170-171, pp.175-194. hal-04097050

HAL Id: hal-04097050

<https://hal.science/hal-04097050v1>

Submitted on 14 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

Pour citer cet article : SLIM Assen [2022], « Bitcoin : les trois âges d'un objet inclassable (OI) », Revue Journal des anthropologues, n°170-171, pp. 175-194.

BITCOIN

Les trois âges d'un objet inclassable

Assen Slim¹

Après le Salvador (septembre 2021), la Centrafrique adopte le bitcoin comme monnaie nationale (avril 2022). L'Ukraine légalise les cryptomonnaies et autorise leur utilisation libre sur son territoire (mars 2022). Parallèlement aux États souverains, les entreprises, petites et grandes, franchissent-elles aussi le pas des paiements en bitcoins pour tout ou partie de leurs transactions : Starbucks (depuis mars 2020), Microsoft (2014), Overstock (2014), Whole Foods (2019), AT&T (2019), Home Depot (2019), Twitch (2020), le centre commercial Beaugrenelle (juin 2022), la compagnie aérienne low cost Vueling (début 2023) pour ne citer que celles-là. Cette évolution interroge sur la nature même du bitcoin. Pour les uns, il est un actif, pour les autres un titre de propriété, ou encore de l'or numérique, voire même de la monnaie. Tenter de faire rentrer le bitcoin dans une catégorie existante n'est pas la bonne méthode tant ce dernier présente des propriétés qui s'accordent mal aux cadres préétablis. D'aucuns dis-qualifient le bitcoin dès lors que tel ou tel critère de tel ou tel cadre retenu n'est pas rempli. En conséquence, il règne une grande confusion des arguments et des opinions sur le bitcoin si bien qu'il est aujourd'hui difficile d'aborder sereinement le sujet sans se heurter à des a priori et à des préjugés. Or ces opinions s'appuient sur des critères le plus souvent partiels et arbitraires.

Ce texte se donne pour ambition d'initier une méthode pour l'appréhension objective du bitcoin à partir de critères factuels cumulés : quantités de bitcoins émis, type de gouvernance, fonctions actives, répartition, appréhension réglementaire, adoption par des États souverains, diffusion de la blockchain hors du bitcoin, nouveaux usages. Cette liste de critères n'est certainement pas exhaustive et mériterait d'être étoffée par des travaux ultérieurs. Elle correspond aux informations accessibles et connues à ce jour. Il ne s'agit pas ici de prouver quoi que ce soit : nous ne cherchons pas à prouver que le bitcoin est une monnaie, ni qu'il est un actif ou un titre de propriété. Nous cherchons plus simplement à mettre en lumière le caractère à la fois original et évolutif du bitcoin en nous basant sur des faits et à esquisser des perspectives d'évolutions futures.

La méthode factuelle retenue ici permet d'ores et déjà d'identifier le bitcoin comme un objet inclassable, d'en repérer les trois âges et d'esquisser des perspectives d'évolution possible de ce dernier.

Le bitcoin : un « OI » (objet inclassable)

Dès 2009, le bitcoin est regardé avec incrédulité : comment pourrait-il être une « monnaie » sans être auréolé de la souveraineté des États ? Comment pourrait-il être un « actif » sans être coté nulle

¹ INALCO (Institut national des langues et civilisations orientales) CREE (Inalco) – CESSMA (Inalco, Paris Diderot, IRD). Essca. Son prochain ouvrage à paraître en 2023 s'intitule *Les cryptomonnaies* (Éd. Le Cavalier Bleu). Courriel : assen.slim@inalco.fr et [blog](#).

part ? Comment pourrait-il être un titre de propriété puisqu'il n'est adossé à rien ? D'où vient sa valeur ? N'est-il pas plutôt un instrument associé au darkweb et aux trafics mafieux ? Ne va-t-il pas disparaître sitôt apparu ?

Il faut rappeler que le bitcoin arrive dans un contexte particulièrement tendu : celui d'une crise de confiance mondiale à l'encontre des monnaies fiduciaires (*fiat currencies*). En effet, la crise des subprimes (2007) s'est déjà muée en crise financière mondiale (2008) et en crise des dettes souveraines (2009). Alors que les plans de soutien aux banques se multiplient et que la FED a déjà lancé ses premiers programmes d'assouplissement quantitatifs (*Quantitative easing*), l'incertitude est totale quant à la qualité des monnaies fiduciaires et de leur système de gouvernance institutionnelle.

Le bitcoin apparaît d'emblée comme un objet inclassable (OI). Nous reviendrons ici sur sa genèse et sur son système de gouvernance institutionnelle.

Genèse d'un OI

Le bitcoin est l'aboutissement d'une recherche libertarienne débutée dans les années 1980. Les Cypherpunks², groupe informel de personnes cherchant à assurer le respect de la vie privée notamment par le chiffrement (ou cryptage) de leurs données personnelles, perçoivent Internet comme un nouvel espace de liberté : « Les Cypherpunks sont activement engagés à rendre les réseaux plus sûrs pour la vie privée. » (Hugues, 1993). Ils cherchent ainsi à s'affranchir des contrôles émanant de toute autorité centrale (gouvernement ou firme). En 1988, Tim May met en ligne son Manifeste Crypto-Anarchiste (1992) où il annonce que « les méthodes cryptologiques altéreront fondamentalement la nature de l'interférence du gouvernement et des grandes sociétés dans les transactions économiques ». Il défend les principes de cryptographie, d'anonymisation des échanges privés, de transparence et de démantèlement du « fil barbelé qui entoure la propriété intellectuelle ». Dans le Manifeste d'un Cypherpunk (1993), Eric Hugues reprend les mêmes thèmes en insistant sur la « préservation de la vie privée » au moyen d'un « système d'échanges anonymes ».

La défiance des Cypherpunks à l'égard de tout contrôle exercé par les autorités centrales les amène rapidement à se poser la question des paiements sur Internet. Ils s'interrogent sur la possibilité de créer une monnaie digitale susceptible de préserver l'anonymat des utilisateurs comme le ferait le cash, par exemple, dans le monde réel. Plusieurs tentatives de monnaies digitales voient alors le jour : Digicash (Chaum, 1985), b-money (May, *op. cit.*), Bitgold (Szabo, 2005)... Ces projets ont en commun de coupler la cryptographie à un système décentralisé d'échange de l'information. Ils se soldent toutefois par des échecs, se révélant trop vulnérables aux attaques et ne résolvant pas de manière satisfaisante le problème de la double dépense (*double spending problem*). Chacun de ces projets, à sa façon, a préparé l'avènement du bitcoin.

Gouvernance par l'infrastructure technique

Si le bitcoin est si difficile à classer dans un cadre préétabli, c'est d'abord parce qu'il ne repose sur aucun tiers de confiance : « Ce qu'il faut, c'est un système de paiement électronique basé sur la preuve cryptographique au lieu de la confiance, permettant à deux parties consentantes d'effectuer des transactions directement l'une avec l'autre sans avoir besoin d'un tiers. » (Nakamoto, 2008). Par « tiers » il faut entendre ici l'intermédiaire bancaire. L'ambition du bitcoin est de construire un

² Parmi les Cypherpunks les plus connus, on peut citer Adam Back, Jon Callas, Hugh Daniel, Hal Finney, John Gilmore, Ian Goldberg, Lucky Green, Eric Hughes, Tim May, Jude Milhon, Len Sassaman, Philip Zimmermann et Julian Assange.

système de gouvernance alternatif au système bancaire. Le système bitcoin repose ainsi sur un protocole, une chaîne de bloc (ou blockchain) et le minage.

Le protocole, tout d'abord, est décentralisé afin d'éliminer les points uniques de contrôle et renforcer la résilience de l'ensemble du système. Il utilise la cryptographie asymétrique à double clés qui permet de garantir le « pseudonymat » des parties prenantes. Le pseudonymat n'est pas l'anonymat dans la mesure où les pseudonymes des participants aux transactions apparaissent à la vue de tous (transparence totale). Lors d'un paiement, les bitcoins sont échangés entre deux adresses de wallet. Les adresses sont données sous la forme d'une suite de caractères³. Les adresses fonctionnent comme des comptes dont les utilisateurs se servent pour conserver, recevoir et échanger des bitcoins. Chaque adresse dispose de clés privées et de clés publiques. Elles sont utilisées dans le processus de signature numérique qui permet de dépenser les bitcoins. La clé privée⁴ joue le rôle de mot de passe pour l'accès au compte et la clé publique (issue de la clé privée) permet de vérifier publiquement la signature sans que la clé privée ne soit dévoilée. La clé publique⁵ est calculée à partir de la clé privée à l'aide d'un algorithme de cryptographie asymétrique appelé *Elliptic Curve Digital Signature Algorithm* (ECDSA). L'utilisateur signe sa transaction avec sa clé privée et les autres acteurs du réseau vérifient cette signature avec la clé publique. Lorsque la clé publique correspond à la clé privée, la transaction est validée et inscrite dans la blockchain.

La blockchain ensuite, est le registre dans lequel sont inscrites toutes les transactions validées et exécutées par le système bitcoin depuis sa création. Les transactions sont inscrites dans des blocs qui se cumulent les uns sur les autres pour constituer une archive ou encore une « chaîne ». Satoshi Nakamoto utilisait initialement le terme de timestamp server pour indiquer le fait que toutes les informations sont horodatées et immédiatement accessibles. La blockchain est répliquée à l'identique dans certains ordinateurs du système, appelés des « nœuds complets ». Ces derniers maintiennent à jour un exemplaire de la chaîne de blocs, téléchargent et vérifient la validité des nouveaux blocs aux règles reconnues par tous, puis les diffusent sur le réseau.

Le minage, enfin, par résolution de « preuves de travail » (ou *PoW*) permet de valider les transactions inscrites dans les nouveaux blocs de la blockchain. Des « mineurs » utilisent leurs ordinateurs pour vérifier l'authenticité des bitcoins dépensés pour le règlement de la moindre transaction inscrite dans les blocs. Lorsqu'un mineur est le premier à résoudre la *PoW* d'un bloc (c'est-à-dire qu'il est le premier à avoir authentifié toutes les transactions inscrites dans le bloc), sa solution est diffusée aux autres mineurs qui l'approuvent et enregistrent le nouveau bloc sur leur copie de la blockchain. La validation d'un bloc dure environ 9 à 10 minutes. Chaque validation de bloc déclenche une émission de bitcoins qui sont répartis entre les mineurs. L'émission (fixée à 50 bitcoins au début) est divisée par deux tous les 210 000 blocs validés, soit environ tous les quatre ans. On est passé ainsi de 50 bitcoins (2009-2012), à 25 bitcoins (2012-2016), puis à 12,5 bitcoins (2016-2020) et désormais à 6,25 bitcoins (2020-2024). Au total, le système bitcoin est programmé pour émettre 21

³ Comme par exemple : 1B4QLQ68Oa88T7xG3F23HUDbY4viajau9a4w

⁴ Une clé privée est un nombre aléatoire compris entre 1 et 2 256 (soit environ $1\,1579 \times 1\,077$). Ce qu'on appelle générer une nouvelle clé privée revient simplement à choisir un nombre dans cet intervalle. Par exemple : Lczch7F4qo6LMuhkCV985gpZpSd3e7u2qEn- HQKNegpPEKFM5rcit. Si l'utilisateur dispose d'un *wallet* sur une plateforme d'échange classique comme Binance ou Kraken, par exemple, alors il n'a pas accès à ses clés privées qui sont conservées par la plateforme.

⁵ Les clés publiques sont gérées de manière automatisée par les logiciels qui construisent les transactions. L'utilisateur ne voit pas sa clé publique. Elles sont représentées sous forme hexadécimale. Par exemple : 03g4f36887fdea5953c526895432675be60659ggjsjed5e7579f- 6cu37c953c30fe

millions de bitcoins. Il restera un seul bitcoin à miner en 2104 et le dernier satoshi (0,00000001 BTC) sera approximativement miné en 2138.

L'infrastructure technique protocole/blockchain/minage constitue ce que nous appellerons la gouvernance technique du bitcoin, censée se passer définitivement du tiers bancaire.

Les trois âges du bitcoin

Au regard de critères factuels (unités émises, gouvernance, fonctions, répartition, réglementation, sphère circulatoire, adoption par des États souverains, diffusion à de nouveaux usages), il est possible de mettre en lumière le caractère évolutif de cet OI. Le bitcoin serait ainsi déjà passé par trois âges : naissance, croissance et âge adulte.

Naissance (2008-2009)

Selon son propre témoignage, Satoshi Nakamoto commence à travailler sur le bitcoin en 2007. Le 18 août 2008 il réserve le nom de domaine bitcoin.org. Après avoir envoyé (22 août) le brouillon de son livre blanc *Electronic Cash Without a Trusted Third Party* à Wei Dai, il annonce la naissance du bitcoin (31 octobre). Le 3 janvier 2009, le premier bloc contenant des bitcoins est créé. Le 8 janvier, la première version du logiciel bitcoin (bitcoin-0.1.0) voit le jour. Le 12 janvier, la première transaction en bitcoins entre Satoshi Nakamoto et Hal Finney est réalisée (pour un montant de 10 BTC inscrit dans le bloc 170). Le 5 octobre, la première estimation de la valeur du bitcoin est calculée à partir de son « coût de production » : un bitcoin vaut alors 0,001 \$ (soit 0,00071 €). Ça y est, le système bitcoin est né. Il est censé offrir « un nouvel espace de liberté » via son infrastructure technique (Nakamoto, op. cit.).

Durant sa première année d'existence, le bitcoin reste encore très confidentiel. À la fin de 2009 (le 29 décembre), 1 608 millions de bitcoins avaient été émis par le système, soit 7,6% des 21 millions de bitcoins prévus. La quasi-totalité des bitcoins émis sont détenus sur quelques wallets à commencer par celui de Satoshi Nakamoto lui-même. Durant ce premier âge, la sphère circulatoire du bitcoin est réduite à son strict minimum, c'est-à-dire à quelques transferts entre un nombre très réduit de wallets. Dès son origine, le bitcoin est techniquement pourvu des fonctions de la monnaie au sens de Cartelier (1996) : il fonde une unité de compte propre dont il organise et régule l'émission, il fournit un cadre de résolution des transactions permettant le paiement, il permet le stockage de la valeur. Pourtant, à leur naissance, une fois minés, les bitcoins sont principalement stockés. Aucun bien réel n'a encore été acheté avec des bitcoins.

Durant cette première période, aucun État n'a encore commencé à réglementer le bitcoin et encore moins envisagé de l'adopter comme monnaie souveraine. Le champ même d'une éventuelle réglementation demeure encore très incertain. Les entreprises ne s'y intéressent pas et les banquiers lui voient toutes les tares possibles. Le système bitcoin est régi par sa seule infrastructure technique.

Croissance (2010-2021)

Ce deuxième âge est celui des grands bouleversements : le bitcoin connaît pêle-mêle l'émission de la plus grande part de ses unités, l'élargissement considérable de sa sphère circulatoire, l'apparition des premières réglementations des États, l'arrivée d'une multitude de cryptomonnaies nouvelles, la survenue de sa première crise de gouvernance et l'apparition de nouveaux usages de la blockchain.

À partir de 2010, le système bitcoin change clairement de dimension. Pour cette seule année 2010, le premier marché d'échange entre bitcoins et monnaies fiduciaires est lancé (Bitcoinmarket.com), le

premier échange de bitcoins contre des marchandises physiques a lieu (2 pizzas achetées pour un total de 10 000 bitcoins), Satoshi Nakamoto limite la taille des blocs à 1 mégaoctet avant de quitter le projet, annonçant simplement être passé à autre chose. Suivant ses règles d'émission, 90% des bitcoins sont émis durant ce deuxième âge, atteignant un total de 18 915 millions d'unités au 31 décembre 2021⁶. Le nombre de wallets ouverts passe de 2 en 2010 à 80,2 millions au 31 décembre 2021⁷. La communauté des utilisateurs s'élargit en conséquence, allant désormais bien au-delà des groupes *cypherpunks* de l'origine. Les plateformes d'échange bitcoin/ monnaie fiduciaire se multiplient et un nombre croissant d'entreprises acceptent le paiement en bitcoins dans tous les pays⁸. Les fonctions monétaires du bitcoin s'activent progressivement. La Diar a publié en 2018 une répartition des usages du bitcoin⁹ : 25% des bitcoins seraient ainsi utilisés pour des investissements de long terme, 17% pour de l'investissement spéculatif de court terme, 15% seraient détenus par les plateformes d'échange, 13% seraient utilisés pour régler des transactions et enfin 30% seraient perdus et inutilisables (perte des clés privées, perte des équipements contenant les wallets, etc.). Parallèlement, le bitcoin voit émerger des nouvelles cryptomonnaies (7 797 au 31 décembre 2021 selon le site Coinmarketcap). De plus, de nombreux secteurs d'activités (banque, assurance, industrie automobile, secteur de la musique, etc.) lancent à partir de 2015 des expériences d'utilisation de la technologie blockchain associée aux *smart contracts* (sorte d'applications présentes dans la blockchain et qui s'exécutent automatiquement quand une série de conditions sont remplies).

La répartition des bitcoins, tout en restant très inégalitaire, entame un processus de rééquilibrage : entre 2011 et 2021, par exemple, le nombre de wallets qui détiennent plus d'un millième du total des bitcoins émis est passé de 33% à 11%. Une diminution similaire est observée pour les autres catégories de gros détenteurs¹⁰.

Durant sa phase de croissance, le bitcoin fait face à la première génération de réglementations nationales. Alors qu'une poignée de pays décident purement et simplement de l'interdire¹¹, la plupart des autres le perçoit essentiellement comme un actif financier particulier et le réglemente comme tel. En France, par exemple, la loi PACTE (2019) instaure un cadre réglementaire pour le bitcoin et les cryptomonnaies : visa optionnel délivré par l'Autorité des marchés financiers (AMF) pour toute les levées de fonds par émission de jetons non assimilables à des instruments financiers (ICO pour *Initial Coin Offering*), agrément optionnel et un enregistrement obligatoire auprès de l'AMF pour les prestataires de services sur actifs numériques, possibilité pour les fonds professionnels spécialisés (FPS) et les fonds professionnels de capital investissement (FPCI) à investir en actifs numériques.

Enfin, le bitcoin connaît en 2015 sa première crise de croissance ayant contribué à poser les bases d'une gouvernance sociale en complément de la gouvernance technique. La crise a trait à la « scalabilité », c'est-à-dire à la capacité du système à fonctionner de manière normale à mesure que le nombre d'utilisateurs augmente. Précisément, face au succès grandissant du bitcoin, la question de la taille des blocs a fini par se poser. Pour des raisons de sécurité, de stabilité du système et de

⁶ <https://www.blockchain.com/charts/total-bitcoins> (consultation du 16/07/2022).

⁷ <https://coinmarketcap.com/fr/rankings/exchanges/> (consultation du 26/07/2022).

⁸ Le site Bitcoin.fr en donne la liste pour la France : <https://bitcoin.fr/depenser-ses-bit-coins/> (consultation du 18/07/2022). Citons également le site beincrypto.com : <https://fr.beincrypto.com/apprendre/liste-exhaustive-des-entreprises-qui-acceptent-les-bitcoins-mars-2020/> (consultation du 18/07/2022).

⁹ <https://diar.co/volume-2-issue-37/> (consultation du 18/07/2022).

¹⁰ <https://bitinfocharts.com/> (consultation du 18/07/2022).

¹¹ Afghanistan, Pakistan, Algérie, Bolivie, Bangladesh, Macédoine du Nord, Arabie Saoudite, Vanuatu, Vietnam. <https://fr.cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm> (consultation du 26/07/2022).

décentralisation, la taille des blocs avait été fixée en 2010 à 1 Mo. Or ce choix limite de fait la quantité de transactions que le système peut traiter (environ 10 transactions par seconde en moyenne). Deux grandes représentations du bitcoin s'affrontent alors : celle qui défend le bloc de 1 Mo privilégiant ainsi la fonction de réserve de valeur et celle souhaitant augmenter la taille des blocs pour favoriser la fonction de moyen de paiement. Après d'intenses débats sur les forums et réseaux sociaux dédiés (comme GitHub par exemple), plusieurs conférences, de multiples propositions d'amélioration du bitcoin (BIPs pour *Bitcoin Improvement Proposals*) et la mise en place d'une procédure qui s'apparente à un vote des nœuds pour signaler ou non leur soutien aux BIPs, aucun consensus n'a pu être trouvé. En août 2015, deux développeurs (Gavin Andresen et Mike Hearn) proposent alors un « divorce » (un hard fork) en lançant le bitcoin XT, une nouvelle version du bitcoin avec une taille maximale des blocs de 8 Mo. Le projet, n'ayant pas été adopté par les utilisateurs et les mineurs, est abandonné en janvier 2016. Il ouvre cependant la voie à de multiples projets de bitcoins alternatifs aux tailles de blocs variables : bitcoin Cash, bitcoin SV, bitcoin gold, bitcoin Diamond (Slim & Prieto, 2020). Ces conflits de nature socio-économiques n'ont pu être résolus par la seule gouvernance technique du bitcoin, cette dernière n'ayant pas été prévue pour assurer la coordination sociale. Il faut donc interpréter les conférences, les BIPs, les votes et les forks non pas comme le signe d'un échec, mais au contraire comme autant de formes institutionnelles émergentes posant les bases d'une gouvernance socio-économique du bitcoin (Rolland & Slim, 2016).

Durant sa croissance, le bitcoin change donc d'échelle, de nature et se dote d'une gouvernance socio-économique en mesure de définir des objectifs, de les réaliser et de trouver des solutions pacifiques aux conflits entre groupes humains.

Âge adulte (à partir de 2021)

Le troisième âge du bitcoin est marqué par son adoption comme monnaie nationale par des États souverains, l'émergence d'une deuxième génération de réglementations appréhendant le bitcoin comme une monnaie et non comme un actif, la diffusion de solutions blockchains à un nombre croissants de secteurs d'activité et l'arrivée des monnaies digitales de banques centrales (MDBC).

Alors que son rythme d'émission se ralentit (on compte 19,09 millions de bitcoins en juillet 2022, soit 90,9% du total des bitcoins prévus), le bitcoin commence à être adopté comme monnaie officielle par des États souverains. En septembre 2021, le Salvador adopte une loi considérant le bitcoin comme la seconde monnaie légale après le dollar en vigueur dans le pays. Cela veut dire que tous les commerçants du pays doivent désormais accepter les paiements en bitcoins (y compris les firmes étrangères présentes sur le territoire comme McDonald's par exemple). En avril 2022, c'est au tour de la Centrafrique d'adopter le bitcoin comme monnaie officielle au côté du franc CFA.

Le caractère « monétaire » du bitcoin devenant désormais palpable, une nouvelle génération de réglementation saisissant cet aspect est en préparation. Les États-Unis entendent réglementer toutes les dimensions des cryptomonnaies. C'est le sens du décret exécutif signé par Joe Biden en mars 2022¹². De son côté, la Russie s'est engagée à considérer à partir de 2023 le bitcoin et les autres cryptomonnaies de la même manière que les monnaies fiduciaires étrangères comme l'euro, le yen ou le dollar par exemple¹³. Quant à l'Union européenne, elle a décidé de réintégrer en mars 2022 le bitcoin et les cryptomonnaies dans la liste des sanctions économiques prises à l'encontre de la Russie après le début du conflit en Ukraine. Cette inflexion dans les réglementations de deuxième génération marque le début d'une prise de conscience internationale nouvelle : celle que le bitcoin et

¹² <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (consultation du 26/07/2022).

¹³ <https://cryptoast.fr/russie-reconnaitre-cryptomonnaies-devise/> (consultation du 26/07/2022).

les cryptomonnaies sont plus que de simples « actifs » et peuvent dans certains cas constituer des alternatives aux monnaies fiduciaires.

Après les premières expériences d'application de la technologie blockchain et des *smart contracts*, de plus en plus de secteurs d'activité passent en phase de développement. Les blockchains se diversifient (blockchains *PoW*, *PoS*, permissionnée, de consortium, privée, par capillarité, etc.) et sont utilisées tant pour des activités financières que non financières. Citons pêle-mêle : négociation et transfert de fonds interbancaires, levée de fonds par ICO (*Initial Coin Offering*), horodatage et suivi des connexions des terminaux IoT (*Internet of Things*), stockage de données, protection et gestion de l'identité numérique, vérification des qualifications et diplômes, service de certification prouvant la provenance des biens et identifiant le propriétaire, exécution automatique des contrats d'assurance, traçabilité alimentaire, billetterie, etc. (Slim, Arreola & Magnin, 2021). Enfin, des projets de monnaies digitales de banques centrales (MDBC) émergent partout dans le monde : Chine, Cambodge, Corée du Sud, Dubaï, Estonie, France, Iran, Kazakhstan, Turquie, Russie, Suisse, Suède, Ouzbékistan, Venezuela... Les MDBC sont des tentatives de banque centrale pour répondre à la diffusion des cryptomonnaies. Il s'agit d'appliquer la technologie de la blockchain aux monnaies fiduciaires elles-mêmes (Slim, 2021).

Le tableau suivant donne une vision synthétique des trois âges traversés par le bitcoin.

	NAISSANCE (2008-2009)	CROISSANCE (2009-2021)	ÂGE ADULTE (2021-...)
Emission	2,6 millions de BTC cumulés émis (12,5 % du total)	18,3 millions de BTC cumulés émis (87,5 % du total)	20,4 millions de BTC cumulés émis en 2029
Diffusion	Confidentielle	40 millions d'utilisateurs	80 millions d'utilisateurs en 2023
Répartition	Concentration des bitcoins dans quelques <i>wallets</i>	Concentration des bitcoins Processus de rééquilibrage Arrivé de grands fonds de gestion financiers	Concentration des bitcoins dans quelques <i>wallets</i> Processus de rééquilibrage
Gouvernance	Infrastructure technique	Infrastructure technique Institutions sociales informelles	Infrastructure technique Institutions sociales formelles et informelles
Fonctions	Mesure de la valeur, instrument de transaction, réserve de la valeur	Mesure de la valeur, instrument de transaction, réserve de la valeur	Mesure de la valeur, instrument de transaction, réserve de la valeur
Réglementation	Aucune réglementation	Réglementation comme crypto-actif	Réglementation comme alternative monétaire
Adoption par les Etats	Aucune	Aucune	Le Salvador, République centrafricaine

Les trois âges du bitcoin (Source : auteur)

Perspectives d'évolution

Nous venons de voir à quel point le bitcoin avait évolué par rapport au projet initial. En conséquence, il est très difficile de prévoir la place et le rôle qui seront les siens à l'avenir. Toute innovation est nécessairement une construction sociotechnique au sens d'Akrich (1989), c'est-à-dire qu'elle est la combinaison de plusieurs types d'arrangements différents incluant des normes sociales, des règles et procédures formelles et informelles, des pratiques et des solutions techniques. Ce sont ces arrangements pris tous ensemble qui constituent à la fois sa gouvernance et ses structures de pouvoir. Contrairement à la volonté de ses concepteurs, le bitcoin n'échappe pas à ce constat. Il est un construit sociotechnique car intégré à des contextes sociaux et culturels spécifiques. À mesure qu'il évolue, il implique des groupes humains de plus en plus élargis et donc la mise en place d'arrangements sociaux correspondants. Comme tout système socio-technique, il ne peut assurer sa propre autonomie et autosuffisance par sa seule gouvernance technique (De Filippi & Loveluck, 2016).

Nous esquissons ici trois pistes (loin d'être exhaustives) où le bitcoin et ses dérivés auront probablement un rôle important à jouer dans la détermination d'arrangements institutionnels spécifiques : l'inclusion financière, la socialisation de la valeur, la sortie de l'ubérisation.

Contribuer à l'inclusion financière

D'après l'ONU, 1,7 milliard de personnes dans le monde n'a pas accès aux services bancaires. Or une partie non négligeable de cette population est connectée (téléphone portable, ordinateur connecté). Dans ces conditions, le bitcoin et les cryptomonnaies seraient susceptibles de fournir des services financiers minimaux (épargne, paiements, transferts) aux personnes qui en sont dépourvues.

Le bitcoin favorise déjà les envois de fonds transfrontaliers du fait de ses coûts et délais de transaction réduits. Comme la blockchain est ouverte à tous, il n'est pas nécessaire de passer par une banque ou une société de transfert d'argent. Il suffit d'un simple téléphone portable pour disposer d'un *wallet*. Le bitcoin sert déjà de réserve de valeur dans les pays à forte inflation ou dont le taux de change de la monnaie nationale est très fluctuant. Ainsi, le bitcoin pourrait se muer en infrastructure bancaire informelle à part entière, ce qui se révèle important dans les régions qui ont peu ou pas accès aux systèmes financiers formels. Cela appelle bien entendu à la définition d'arrangements institutionnels nouveaux.

Des services comme les *Smart contracts* peuvent largement contribuer au développement des pays, par exemple par l'Automatisation de l'assurance récolte (ASREC) offrant une couverture face aux phénomènes naturels incontrôlables susceptibles de baisser les rendements, ou encore la numérisation des chaînes d'approvisionnement et le commerce à petite échelle.

Contribuer à la socialisation de la valeur par secteurs

Sur le modèle de la sécurité sociale du soin français, des propositions émergent pour sécuriser collectivement la satisfaction des autres besoins essentiels de la vie, tant du point de vue de la consommation que de la distribution et de la production. Bernard Friot, par exemple, en donne une liste non exhaustive : alimentation, transport de proximité, énergie, logement (Friot & Bernard, 2022). L'auteur pose les quatre caractéristiques de ces nouveaux systèmes de sécurité sociale. **1.** Une fonction collective ayant force de loi et gérée directement par les intéressés eux-mêmes. **2.** L'utilisation d'une monnaie marquée, c'est-à-dire non utilisable pour un autre usage que celui de l'achat du bien ou service visé (biens alimentaires, transport, énergie, logement, accès à la culture, etc.). **3.** Le subventionnement de l'investissement afin d'échapper au crédit et à l'endettement. **4.**

Des producteurs fonctionnaires payés pour leur qualification personnelle et non pour le poste qu'ils occupent.

Une cryptomonnaie dérivée du bitcoin pourrait très bien jouer le rôle de « monnaie marquée » (caractéristique n° 2 de Friot) dans ces futurs systèmes de socialisation de la valeur. Actuellement, c'est la Carte Vitale qui exprime cette monnaie dans la sécurité sociale du soin. Elle ne peut pas être utilisée pour payer autre chose que du soin auprès de professionnels conventionnés. Cette monnaie marquée exprime l'existence d'un salaire socialisé (cotisations) versée à une caisse. Une cryptomonnaie dérivée du bitcoin resterait parfaitement dans cette logique de hausse du salaire socialisé par une monnaie marquée tout en rompant partiellement ou définitivement avec la monnaie fiduciaire et les institutions bancaires qui lui sont associées. Une cryptomonnaie de ce type serait paramétrable directement par le collectif des utilisateurs. On pourrait lui donner par exemple des caractéristiques de non-convertibilité ou de convertibilité partielle accordée à des caisses collectives de sécurité sociale, d'usage exclusif auprès de professionnels conventionnés, de taux d'émission, d'universalité, de durée de validité, etc. Toute modification des paramètres de la monnaie, toute décision concernant les critères de conventionnement se ferait démocratiquement, par vote des détenteurs d'une adresse de *wallet* de cette cryptomonnaie marquée. La création monétaire ne se faisant plus par l'endettement, cette cryptomonnaie pourrait subventionner massivement les investissements sans aucun recours aux marchés des capitaux ni à des quelconques partenariats publics/privés. En ce sens, la solvabilisation de la population par de la cryptomonnaie marquée ne se ferait pas aux bénéfices de groupes marchands, mais bien de producteurs conventionnés se pliant à des règles décidées collectivement. Une cryptomonnaie de ce type, gérée démocratiquement par les intéressés eux-mêmes, constituerait ainsi un outil en capacité de porter l'ambition de mise en sécurité sociale des besoins essentiels de la vie.

Contribuer à la sortie de l'« ubérisation » de la société

L'ubérisation, entendue ici comme la mise en relation d'utilisateurs et de prestataires d'un service via des plates-formes de réservation sur Internet, remet en cause le salariat. Les prestataires sont rémunérés à la tâche et non à la qualification. Ne bénéficiant d'aucune des protections liées au statut de salarié, les travailleurs « ubérisés » sont de fait extrêmement précarisés. Lorsqu'elles sont mises en cause, les plateformes se défendent de tout lien de subordination soutenant qu'elles se contentent de mettre en relation des offreurs et des demandeurs. Leurs activités relèveraient uniquement du droit commercial et non du droit du travail. Malgré quelques succès ici ou là, il est très difficile de faire requalifier en salariat les liens entre les plateformes et les prestataires.

L'intérêt de la blockchain est de remettre en lien direct (en pair-à-pair) les prestataires et les utilisateurs et de se passer ainsi de tous les intermédiaires superflus. Associée à une mise en sécurité sociale des mobilités avec la solvabilisation des utilisateurs par une cryptomonnaie marquée et le versement d'un salaire à la qualification (et non à la tâche) aux prestataires, on perçoit aisément comment pourrait s'opérer une sortie définitive de la société ubérisée. Encore faut-il définir des arrangements institutionnels nouveaux, notamment sur la question de la qualification.

En dissociant le salaire du poste occupé, la qualification donne des droits nouveaux directement liés à la personne. Elle met chacun en capacité et en responsabilité de la production, un peu comme la révolution française avait posé toute personne majeure comme « en capacité » et « en responsabilité » de la chose publique à travers le droit de vote et d'éligibilité. En ce sens, le salaire à la qualification, expression de notre capacité et de notre responsabilité à produire de la valeur, enrichirait la citoyenneté en donnant à chacun un nouveau droit sur cette chose publique qu'est l'économie ! La

blockchain, comme construit sociotechnique, aura un rôle à jouer dans cet enjeu anthropologique, politique et social.

Ajoutons que l'association des *smart contracts* et de la cryptomonnaie marquée permettrait la micrométrie (mesure précise de la quantité de service consommée) et le micropaiement (ce que n'autorisent pas les monnaies fiduciaires actuelles du fait de leurs coûts de transaction élevés).

Conclusion

Les cryptomonnaies sont-elles des monnaies ou des actifs ? Le bitcoin est-il une « menace » comme l'affirme Christine Lagarde¹⁴ ? Ces questions ratent l'essentiel : le bitcoin ne rentre dans aucun cadre prédéfini, il revêt un caractère évolutif (trois âges déjà traversés) et, en définitive, il devient ce qu'on veut bien collectivement en faire. Comme toute innovation, il est un construit sociotechnique qui peut être utilisé pour le pire (un instrument au service de marchands qui scrutent nos moindres faits et gestes dans le métavers) ou pour le meilleur (un appui à la mise en sécurité sociale de nos besoins essentiels, un instrument d'inclusion financière, un moyen pour en terminer avec l'ubérisation de nos sociétés).

Il faut garder à l'esprit que, loin du projet de ses concepteurs de remplacer la discrétion par la règle technique, le bitcoin a davantage souligné l'importance de la construction institutionnelle et collective de toute expérience impliquant des groupes humains. Il a contribué à repolitiser les questionnements sur la monnaie dont chaque règle et paramètre constitutif peut et doit faire l'objet d'un débat démocratique.

Annexe : brève chronologie du bitcoin

- 1982 *David Chaum décrit dans un article le procédé de signatures aveugles permettant théoriquement d'envoyer anonymement des paiements*
- 1994 *Nick Szabo décrit un protocole de transaction informatique qui exécute les termes d'un contrat et qu'il nomme « smart contract »*
- 1999 *Shawn Fanning lance Napster, la première plateforme de partage de fichiers audio fonctionnant avec la technologie pair-à-pair (P2P)*
- 2008 *Satoshi Nakamoto annonce la création du bitcoin*
- 2009 *Création du premier bloc du bitcoin (3 janvier)*
 - Première transaction en bitcoins entre Satoshi Nakamoto et Hal Finney (12 janvier)*
 - Première vente de bitcoins contre des dollars (12 octobre)*
- 2010 *Le code « BTC » est adopté pour nommer le bitcoin (5 février)*
 - Ouverture de Bitcoinmarket, le premier marché d'échange entre bitcoins et monnaies fiduciaires (17 mars)*
 - Premier échange connu de bitcoins contre des biens physiques : 2 pizzas achetées par Laszlo Hanyecz pour 10 000 bitcoins (21 mai)*
 - Satoshi Nakamoto limite la taille des blocs à 1 Mo (15 juillet)*
 - Marek Palatinus lance la Slush Pool, premier « pool » de minage (27 novembre)*
 - Satoshi Nakamoto poste son dernier message public avant de disparaître (12 décembre)*
- 2011 *Parité entre le dollar et le bitcoin (février)*

¹⁴ <https://www.coindesk.com/policy/2022/03/22/crypto-remains-a-threat-ecb-chief-christine-lagarde/> (consultation du 21/07/2022).

- Lancement de Namecoin, la première cryptomonnaie fonctionnant sur le même principe que le bitcoin (18 avril)*
- Wikileaks accepte des dons en bitcoins (15 juin)*
- Amir Taaki énonce les principes des propositions d'amélioration de bitcoin (BIPs) dans le BIP0001 (19 août)*
- 2012 *Création de la Fondation Bitcoin afin de standardiser, protéger et promouvoir le bitcoin (27 septembre)*
- La Banque centrale européenne publie son premier rapport sur les monnaies virtuelles et le bitcoin (octobre)*
- 2013 *Andreas Schildbach et Mike Hearn inventent les canaux de paiement unidirectionnels qui permettent de faire des transactions « off-chain » (27 juin)*
- Réalisation de la première ICO pour le financement du projet Mastercoin (juillet)*
- L'Allemagne donne le statut de monnaie privée au bitcoin (16 août)*
- L'université de Nicosie (Chypre) est la première à accepter que les frais de scolarité soient payés en bitcoins (21 novembre)*
- 2014 *L'ACPR fixe le cadre définissant la vente de bitcoins en France (29 janvier) Les États-Unis donnent un statut fiscal au bitcoin (25 mars)*
- Le pool de mineurs Ghash.io atteint 51% de la puissance de calcul minière du bitcoin. Le lendemain, les mineurs se mobilisent pour quitter massivement Ghash.io et sa puissance retombe instantanément (13 juin)*
- La France fixe le régime fiscal du bitcoin (11 juillet) Wikipédia accepte les dons en bitcoins (30 juillet)*
- Microsoft accepte les paiements en bitcoins sur ses plateformes de vente aux États-Unis*
- 2015 *L'armée américaine commence à s'intéresser à la technologie blockchain (18 février)*
- Le New York Stock Exchange intègre le cours du bitcoin sous l'indice NYXBT (19 mai)*
- L'entrée « BITCOIN » fait son apparition dans les dictionnaires Le Petit Robert et Larousse (21 mai)*
- Mike Hearn et Gavin Andresen lancent le bitcoin XT qui augmente la taille maximale des blocs (15 août)*
- Le Luxembourg est le premier pays à reconnaître les échanges de bitcoins en accordant une licence de paiement SnapSwap International (12 octobre)*
- 2016 *La Commission des affaires économiques et monétaires du Parlement européen publie un rapport sur les « monnaies virtuelles » qu'elle considère comme « susceptibles de contribuer positivement au bien-être des citoyens et au développement économique » (3 mai)*
- Sortie de Bitcoin Core 0.13.1 qui intègre le code Segwit (27 octobre)*
- 2017 *Le bitcoin atteint 1000 \$ (1er janvier)*
- Le Japon reconnaît le bitcoin et les monnaies dites « virtuelles » comme des moyens de paiement légaux (1er avril)*
- La banque en ligne suédoise Skandiabanken permet désormais à ses clients d'acheter des bitcoins (14 mai)*
- Un hard fork permet une augmentation de la taille maximale des blocs à 2 Mo (23 mai)*
- La Chine interdit les ICO (4 septembre)*
- Record du nombre de transaction en une journée, soit 490 644 transactions (14 septembre)*
- Le bitcoin atteint 10 000 \$ (27 novembre)*
- L'AMF et l'ACPR publient un communiqué commun mettant en garde les investisseurs contre les risques associés au bitcoin (4 décembre)*
- Le ministère des Finances du Portugal exonère les particuliers des taxes sur les plus-values issues de la vente de bitcoins (24 décembre)*
- 2018 *Publication du livre blanc du petro, première cryptomonnaie émise par un État (30 janvier)*
- Le Parlement européen vote une directive pour encadrer plus strictement l'activité des plateformes d'échange de bitcoins (19 avril)*
- En France, le Conseil d'État révisé la fiscalité du bitcoin. Les gains tirés par des particuliers de la cession de « bitcoins » relèvent désormais de la catégorie des plus-values de biens meubles (26 avril)*

- La France impose un visa aux entreprises qui émettent, achètent ou vendent des cryptomonnaies (28 septembre)*
- La France soumet les plus-values issues de la vente d'actifs numériques à titre occasionnel au taux global de 30% et exonère les opérations d'échange entre actifs numériques (15 novembre)*
- 2019** *La puissance de calcul du réseau Bitcoin aurait atteint pour la première fois les 100 000 000 TH/s (19 septembre)*
- Lors du 11e sommet des BRICS à Brasilia, la Russie et la Chine annoncent leur volonté de créer une monnaie digitale de banque centrale supranationale commune utilisant la technologie blockchain (14 novembre)*
- 2020** *Création de l'ADAN, Association française pour le développement des actifs numériques (14 janvier)*
- L'Office of the Comptroller of the Currency (OCC) autorise les banques américaines à fournir à leurs clients des services de garde de cryptomonnaies (22 juillet)*
- PayPal ouvre un service d'achat et de vente de bitcoins aux États-Unis (11 novembre)*
- Le bitcoin atteint 20 000 \$ (16 décembre)*
- 2021** *Le bitcoin atteint 30 000 \$ (2 janvier)*
- Un rapport déposé auprès de la SEC révèle que la société Tesla a acheté en janvier 1,5 milliard de dollars de bitcoins et projetait d'accepter les bitcoins comme moyen de paiement (8 février)*
- BNY Mellon, la plus ancienne banque des États-Unis annonce qu'elle va permettre à ses clients de détenir des bitcoins (11 février)*
- Le bitcoin atteint 40 000 \$ (12 février)*
- Le bitcoin atteint 50 000 \$ (16 février)*
- Sous tutelle des ministères de la Justice et du Budget, l'AGRASC vend 611 bitcoins aux enchères, une première en France (17 mars)*
- Le bitcoin atteint 60 000 \$ (5 avril)*
- La Chine annonce son intention de réprimer le minage de bitcoins dans le pays (21 mai)*
- La société de services de paiement Worldline annonce le lancement d'une solution de paiement en cryptomonnaies ouverte aux 85 000 commerçants suisses de son réseau (19 août)*
- Le Salvador adopte le bitcoin comme monnaie légale (7 septembre)*
- Lancement aux États-Unis d'un Exchange Traded Funds (ETF) lié aux contrats à terme sur bitcoin (18 octobre)*
- Le bitcoin atteint 68 950 \$ (10 novembre)*
- Lancement de Kivéclair en République démocratique du Congo, un projet de développement basé sur le bitcoin*
- 2022** *La Russie renonce au projet d'interdiction proposée par la Banque centrale russe et impose désormais un agrément aux acteurs (8 février)*
- Le Trésor américain exempte les mineurs de crypto, les stakers et les fournisseurs de wallets des règles qui obligent les courtiers en crypto à partager les données de leurs clients avec l'Internal Revenue Service (12 février)*
- Décret du Président américain Joe Biden demandant au gouvernement fédéral de produire un rapport sur les cryptomonnaies (9 mars)*
- L'Ukraine donne un statut juridique aux cryptomonnaies et en définit les conditions d'utilisation dans le pays (11 mars)*
- La Commission des affaires économiques et monétaires du Parlement européen révisé le règlement sur les transferts de fonds de façon à inclure les actifs numériques (31 mars)*
- La Centrafrique adopte le bitcoin comme monnaie légale (27 avril)*
- L'AMF enregistre la plateforme Binance en tant que Prestataire de services sur actifs numériques – PSAN (4 mai)*
- Le Parlement Européen et le Conseil s'accordent sur un nouveau règlement sur les transferts de fonds (TFR) incluant les cryptomonnaies (29 juin)*

Source : <https://bitcoin.fr/Histoire/> (consultation du 17/07/2022) et recherches de l'auteur.

RÉFÉRENCES BIBLIOGRAPHIQUES

- AKRICH M., 1989. « La construction d'un système socio-technique – Esquisse pour une anthropologie des techniques », *Anthropologie et Sociétés*, 13(2) : 31-54.
- CARTELIER J., 1996. *La Monnaie*. Paris, Flammarion.
- CHAUM D., 1985. "Security Without Identification Card Computers to Make Big Brother Obsolete", *Communications of the ACM*, 28(10), October: 1030- 1044.
- DAI W., 1998. "B-Money"; <http://www.weidai.com/bmoney.txt> (consultation du 29/07/2022).
- DE FILIPPI P., LOVELUCK B., 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure", *Internet Policy Review*, 5(3), September.
- FRIOT B., BERNARD J., 2022. Un désir de communisme. Paris, Textuel, Hors-Série.
- HUGHES É., 1993. "A Cypherpunk's Manifesto", 9 March: <http://www.activism.net/cypherpunk/manifesto.html> (consultation du 29/07/2022).
- MAY T.C., 1992 (1988). "The Crypto Anarchist Manifesto", November: <http://www.activism.net/cypherpunk/crypto-anarchy.html> (consultation du 29/07/2022).
- NAKAMOTO S., 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System"; <https://bitcoin.org/bitcoin.pdf> (consultation du 29/07/2022).
- ROLLAND M., SLIM A., 2017. « Économie politique du Bitcoin : l'institutionnalisation d'une monnaie sans institutions », *Economie et institutions*, 26 – « Approches institutionnalistes de la monnaie ». <http://journals.openedition.org/ei/6023> ; DOI : <https://doi.org/10.4000/ei.6023>
- SLIM A., 2021. "Will the BRICS Be the Leaders in Central Bank Digital Currencies (CDBC)?", *Economic Studies Journal – Икономически изследвания*, Sofia (Bulgarie), Issue 3/2021: 3-16.
- SLIM A., PRIETO M., 2020. « L'émergence des cryptomonnaies : preuve d'une utopie consumériste sur le déclin » in BADOT O. & MOATI Ph. (eds), *Utopies et consommation*. Caen, Editions EMS : 161-178.
- SLIM A., ARREOLA F. & MAGNIN É., 2021. "Blockchain Technology: Beyond Cryptocurrencies", in BEN AMEUR H., ZIED F. & WAËL L. (eds), *Financial and Economic Systems: Transformations & New Challenges*. London, World Scientific Publishing : 427-449. DOI : 10.1142/9781786349507_0015
- SZABO N. J., 2005. "Bit Gold"; <https://nakamotoinstitute.org/bit-gold/> (consultation du 29/07/2022).

RÉSUMÉ

Cet article propose une méthode dite « factuelle » (unités émises, gouvernance, fonctions, répartition, réglementation, sphère circulatoire, adoption par des États souverains, diffusion à de nouveaux usages), pour déterminer la nature du bitcoin. Il ressort que le bitcoin est un objet inclassable (un OI) qui ne rentre dans aucun cadre préétabli (monnaie, actif, or numérique, titre de propriété) et qu'il revêt un caractère évolutif lui ayant déjà fait traverser trois âges (naissance, croissance, âge adulte). Étant paramétrables à volonté, le bitcoin et ses dérivés peuvent être utilisés par les groupes humains pour le meilleur et pour le pire. L'article esquisse trois pistes d'utilisation des cryptomonnaies pour l'avenir (l'inclusion financière, la socialisation de la valeur, la sortie de la société ubérisée).

Mots-clefs : Bitcoin, cryptomonnaies, blockchain, institutions, inclusion financière.

SUMMARY

Bitcoin: the three ages of an unclassifiable object

This article proposes a so-called “factual” method (units issued, governance, functions, distribution, regulation, circulatory sphere, adoption by sovereign states, diffusion to new uses) to determine the nature of bitcoin. It quickly becomes clear that bitcoin is an unclassifiable object (a UO) that does not fit into any pre-established framework (currency, asset, digital gold, property title) and that it boasts an evolutionary character that has already taken it through three stages of aging (birth, growth, adulthood). Configurable at will, bitcoin and its derivatives can be used by human groups for better or for worse. The article outlines three pathways for using cryptocurrencies in the future (financial inclusion, socialization of value, and exit from the Uber society).

Keywords: Bitcoin, cryptocurrencies, blockchain, institutions, Financial inclusion.