École des Hautes Études en Sciences Sociales

Ecole doctorale de l'EHESS

Centre d'Étude des Mouvements Sociaux (CEMS)

Discipline : Économie et Sciences sociales

ROLLAND MAËL

LIVRET 2 : GLOSSAIRE & ANNEXES

GLOSSAIRE : CRYPTOMONNAIE ET PROTOCOLE DE REGISTRE DISTRIBUÉ

Les termes explicités dans le glossaire se trouvent présentés en italique, suivis d'un astérisque (*) et explicités brièvement pour leur première occurrence dans le manuscrit. Après, ils ne seront plus suivis que d'un astérisque (*). Sources principales : Rauchs et al, 2018 ; Bano et al, 2017 ; Seibold et Samman, 2016 ; adaptations et compléments de l'auteur.

[Français | Anglais : définition] : les termes en français sont accompagnés de leurs équivalents en anglais, qui prédominent dans le domaine étudié, imposant certains concepts et notions sous leur forme anglaise comme points de référence et de connaissance commune. Ce sont ces termes que nous utiliserons par la suite (par exemple, *Fork**, *smart contract).*

Actif digital | Digital Asset :

L'appellation « actif digital* » est le terme le plus englobant, ne se limitant pas aux technologies de registre* distribué. Elle inclut également toutes les formes d'actifs et monnaies sous forme numérique, comme les points de fidélité, les accessoires et skin dans un jeu, etc., qui sont aussi des actifs de ce type. Voir encadré Chap.II.3.

Administrateur | Administrator :

Parmi les « Core Développeurs* », correspond à l'ensemble des acteurs disposant de droits privilégiés au sein du répertoire de dépôt du code source du logiciel référent, hébergé sur une *forge logicielle**. Suivant les niveaux de privilèges, les administrateurs peuvent ajouter, supprimer et modifier le code source.

Algorithme de consensus | Consensus Algorithm :

Correspond à l'ensemble de règles et processus utilisés par les participants afin de vérifier, traiter et parvenir à un accord sur un enregistrement canonique*, gage du maintien dynamique de la cohérence* des données endogènes*. Il en existe différentes familles - Preuve de travail* (PoW*), Preuve d'enjeu* (PoS), Preuve d'enjeu déléguée (DPoS), etc. Ce terme renvoie d'abord à l'algorithme utilisé au sein de la famille *PoW** pour valider un nouvel enregistrement candidat* (Sha 256, Scrypt, etc.).

Altcoin | Altcoin :

La dénomination indigène Altcoin regroupe et qualifie péjorativement toutes les cryptomonnaies*, actifs numériques et monnaies digitales*, à l'exception du Bitcoin, pris comme idéal-type. Certains termes utilisés par des figures communautaires dites Maximalistes* sont encore plus péjoratifs (scamcoin ; shitcoin, etc...) et mettent en évidence les différences et les critiques philosophiques et pratiques qui structurent ces communautés.

Archivage partagé | Shared recordkeeping :

Désigne la capacité du système à permettre à plusieurs parties de créer, entretenir et mettre à jour collectivement un ensemble d'enregistrements partagés.

Arbre de Merkle (ou de Hachage) | Merkle tree (or Hash Tree) :

Correspond à une méthode cryptographique permettant de structurer des données d'un volume souvent important, via des *empreintes numériques**. Elle permet d'accéder à un ensemble de données et d'en vérifier l'intégrité, réduites à des *Hash** sans avoir à les posséder elles-mêmes dans leur totalité. Un arbre de hachage est constitué par un ensemble d'empreintes numériques interdépendantes où les feuilles sont le *hash** de chacun des blocs de données initiales, et qui, concaténés deux à deux, permettent de calculer un hash* parent. Ces *hash** parents sont eux-mêmes concaténés deux à deux jusqu'à l'obtention d'un *hash** unique qui correspond au hash*-sommet ou racine (« *Merkle root* »). Ce dernier est donc une empreinte liée cryptographiquement à toutes les empreintes des données initiales. Dans le cas d'une cryptomonnaie*, cette racine, intégrant la totalité des hash* des transactions* contenues dans un *enregistrement**, se trouvera dans l'*en-tête du bloc**. Voir Annexes n°V.4.

Au sein du protocole | On Chain :

Interactions, transactions*, processus qui se produisent au sein des frontières formelles du protocole de registre* distribué et qui se retrouvent représentées dans la couche de données du système.

Authentification cryptographique | Cryptographic authentification :

Processus permettant de prouver l'identité des contreparties, l'existence et la possession d'actifs digitaux *via* des couples de clefs publiques et

privées (voir aussi *signature cryptographique*). Voir Annexes n°V.1 et V.2.

Chaîne de blocs | Blockchain :

L'usage du terme Blockchain est une synecdoque particularisante réduisant le tout à une de ses parties, en l'espèce à la structure de données. Ce concept, popularisé par des slogans comme « Forget Bitcoin, embrace Blockchain » émanant d'acteurs de la finance traditionnelle (en l'espèce Blythe Master de JP Morgan), reste discutable, car il invisibilise l'essentiel, à savoir le protocole qui le soutient et le rôle incitatif du monnayage et de l'unité de compte native émise dans la production d'un consensus. D'ailleurs, certains protocoles de registre* distribué reposent sur des familles de structure de données différente, très éloignée de cette structure en enregistrements* ou Blocs (les DAG pour « Directed Acyclic Graph », par exemple).

Cible de difficulté | Difficulty target :

Dans un consensus basé sur la *preuve de travail**, il s'agit d'un seuil à atteindre pour que l'*empreinte numérique* de l'*en-tête d'un enregistrement candidat* soit considérée* comme valide (être inférieur ou égal). Cette cible de difficulté est programmée pour augmenter ou diminuer afin de maintenir un *temps d'enregistrement**.

Code Source Ouvert | Open Source Code :

Le code source de l'implémentation logicielle est accessible au public et ouvre, suivant les droits accordés, à des modifications et à des copies, contrairement au code propriétaire, non accessible au public et couvert par des droits de propriété intellectuelle.

Cohérence | Consistency :

Propriété recherchée par tout système informatique de calcul distribué permettant que tous les nœuds* du système accèdent exactement aux mêmes *données endogènes**. Aucune cryptomonnaie n'est cohérente à un instant T et cette propriété renvoie à la probabilité (forte ou faible) que le système parvienne à un consensus sur une valeur proposée. C'est l'*algorithme de consensus** qui lève à court terme l'ambiguïté, forçant l'ensemble des nœuds* du réseau* à converger sur une histoire commune qu'ils dupliquent et sur laquelle ils continuent à enregistrer les changements d'état.

No Coiners*vs* Coiners | No Coiners *vs* Coiners :

Termes indigènes servant à caractériser les acteurs relativement à leurs possessions ou non de CM et crypto-actifs*. Le terme No Coiner fut premier : il sert à qualifier péjorativement les personnes ne possédant pas de Bitcoin ou d'Altcoin* et qui, dans le même temps, expriment scepticisme et critique à leur encontre. À l'opposé et en symétrie, le terme « Coiners* » ou « crypto bro » est venu qualifier ceux qui possédant des CM, les défendent à tout prix.

Confirmation | Confirmation :

Correspond au nombre d'enregistrements successifs « minés » au-dessus du bloc d'une transaction* considérée. Ce nombre indique également combien d'enregistrements doivent être inversés ou écrasés pour supprimer une transaction* du registre. La finalité d'une transaction* renvoie à un nombre de confirmations considéré comme suffisant pour s'assurer d'un règlement irréversible. Sur Bitcoin, c'est généralement 6 confirmations qui sont attendues aujourd'hui.

Contrat intelligent | Smart-contract (SC) :

Voir script à exécution programmatique.

Consensus multi-parties | Multi-party Consensus :

Désigne la capacité d'un système de protocole de registre* distribué à arriver à un accord entre différentes parties prenantes sur un ensemble partagé d'enregistrements faisant autorité et ce, en l'absence d'une autorité centrale.

Cryptographie (ou chiffrement) | Cryptography :

Correspond à une discipline qui s'intéresse à un ensemble de techniques et d'algorithmes permettant de chiffrer/déchiffrer des informations. Loin de ne faire que « cacher », les outils cryptographiques permettent, par chiffrement, la certification et l'authentification de données (signature par clef privée, déchiffrement/vérification par clef publique), comme des voies de structuration des données (les *fonctions de hash**, *arbre de Merkle**).

Crypto-actifs | Crypto Assets :

Les crypto-actifs* sont des objets numériques dont la matérialité, bien qu'inscrite dans un protocole de registre* distribué, repose sur un ou plusieurs centre(s) établi(s), reconnu(s) et disposant de droits exorbitants. Comme tout actif financier, ces formes suivent une logique contractuelle de signature et, en cela, se rapprochent des titres financiers. Voir encadré Chap.II.3.

Cryptomonnaie (CM) | Cryptocurrency :

Les CM recouvrent les UCN* émises et administrées par des protocoles de registre* distribué publics et s'apparentent à une nouvelle catégorie de monnaie, suivant leur gouvernance

singulière qui les voit reposer ni sur la logique de signature propre à la finance, ni sur la logique de sceau propre aux monnaies nationales. Bien que collective, cette logique de co-monnayage distribué est fondée sur un consensus entre l'ensemble des participants d'où une transparence, une sécurité et une intégrité du système qui ne reposent pas sur une autorité centrale, mais sont polycentriques. Voir encadré Chap.II.3.

Débit | Throughput :

Le débit représente le taux maximum auquel un protocole de registre* distribué peut traiter des transactions*, généralement mesuré en transactions* par seconde (TPS). Il dépend de divers facteurs, tels que le type d'algorithme de consensus* ou la taille des blocs de données. Un débit élevé est crucial pour la scalabilité et la performance des systèmes de registre* distribué.

Développeurs | Developpers :

Correspond à l'ensemble des acteurs qui, suivant leurs compétences spécifiques, peuvent écrire et relire les codes informatiques qui sous-tendent les éléments technologiques constitutifs des systèmes de protocoles de registre* distribué (couche protocolaire) et/ou de leurs systèmes connectés (couche applicative). Ils peuvent être professionnels ou participer comme contributeurs bénévoles.

Disponibilité | Availability :

Correspond à une propriété recherchée par tout protocole de registre* distribué permettant de garantir que toutes les requêtes soient satisfaites et que les *données endogènes** soient toujours disponibles.

Données endogènes | Endogenous references :

Correspondent aux données pouvant être créées et transférées uniquement par le biais du protocole de registre* distribué et qui, par leur format, leur sémantique, etc., ont un sens en son sein. Essentielles à son fonctionnement, elles garantissent la cohérence et l'intégrité des transactions* et des enregistrements. Par exemple, pour Bitcoin et Ethereum, les données endogènes incluent les transactions*, les blocs et les contrats intelligents.

Empreinte numérique | Hash :

Voir fonction de hachage.

Enregistrement candidat | Candidate Record :

Correspond à un enregistrement fraîchement propagé au réseau* et donc, qui ne fait pas encore l'objet d'un consensus en son sein. C'est lorsqu'une majorité de nœuds* l'ont reçu, vérifié et intégré dans leur registre* transactionnel qu'il s'érige en *enregistrement canonique**

Enregistrement canonique | Record :

Un enregistrement - pour Bitcoin et Ethereum, il est d'usage de le nommer « Bloc » - représente un ensemble de données de transaction* conteneurisé, reconnu par l'ensemble des nœuds* comme canonique, après que chacun en a vérifié la validité. Un enregistrement est composé d'un *en-tête de bloc** et de la liste des transactions* qu'il contient, c'est-à-dire des transactions* traitées et validées depuis le bloc précédent, à laquelle s'ajoute la plupart du temps une transaction* attribuant une récompense au créateur de cet enregistrement.

Enregistrement de genèse | Genesis Record (or Genesis Block) :

Il correspond au premier enregistrement émis et diffusé au sein d'un protocole de registre* distribué. Il a un statut particulier puisqu'il ne peut faire référence à un enregistrement précédent, contrairement aux autres enregistrements, ni à aucune transaction* lui ayant précédé. Le bloc de genèse est codé dans les logiciels originaux et lance le protocole.

En-tête d'enregistrement (ou de bloc) | Record header (or block header) :

Un en-tête d'enregistrement est unique et sert à identifier un enregistrement particulier sur un *registre**. C'est cet en-tête d'enregistrement qui est haché lors du processus de *preuve de travail**. Sous le protocole Bitcoin, les *enregistrements* ou* blocs sont composés d'un en-tête de taille fixe contenant les informations uniquement nécessaires pour l'assemblage du registre* (ou *blockchain*). Bien que cette taille très limitée ne permette pas de stocker l'ensemble des transactions*, l'en-tête contient néanmoins la racine d'un *Arbre de Merkle**, ce qui permet de vérifier la présence d'une transaction* spécifique dans le *registre** sans avoir à en télécharger l'intégralité.

Évolutivité ou Mise à l'échelle | Scalability :

Capacité d'un système de protocole de registre* distribué à gérer un nombre croissant d'interactions de manière efficace sans compromettre ses performances.

Explorateur de registre | Ledger explorer :

Correspond à un outil offrant une interface utilisateur pour visualiser les données en temps réel d'un protocole de registre distribué. Facilitant la transparence et la vérification des transactions*, il s'agit d'un outil *off chain* essentiel pour les utilisateurs et les développeurs* qui souhaitent suivre l'activité et la santé du réseau*.

Frais de transaction au sein de la chaîne | On chain transaction fees finality :

Ce sont des frais exprimés et payés en *unité de compte native**, que définit l'utilisateur lorsqu'il produit une transaction* afin d'interagir au *sein de la chaîne**. Généralement, et par-delà les différences entre les CM et leurs mécanismes de frais, la quantité de frais de transaction* payée relativement aux autres usagers détermine la rapidité avec laquelle cette transaction* sera traitée : les *opérateurs de transaction** ont tendance à choisir de traiter les transactions* ayant les frais les plus élevés, de fait les plus rentables, puisque ces frais de transaction* s'ajoutent à la *récompense d'enregistrement* pour constituer le revenu d'activité des *opérateurs de traitement des transactions**. L'utilisation de *passerelles** (bourse d'échange, etc.) peut induire, en plus de frais de transaction* au sein de la chaîne, des frais de transaction* en dehors de la chaîne, définis par les conditions générales de vente de la passerelle*.

Finalité de la transaction | Transaction finality :

Désigne le moment où un enregistrement confirmé peut être considéré comme définitif et irréversible. Elle peut être probabiliste, comme avec la PoW* de Bitcoin, où la réversibilité devient computationnellement impossible après quelques blocs. Elle peut aussi être explicite, avec des protocoles intégrant des points de contrôle. En général, ce sont les acteurs économiques acceptant les unités de compte natives (UCN*) qui définissent le nombre de confirmations nécessaires pour considérer une transaction* comme réglée de leur côté.

Fonction de hachage | Hash fonction :

Correspond à une fonction cryptographique qui, appliquée à des données brutes entrantes, les chiffre sous la forme d'une empreinte numérique* unique et partielle (un ***Hash****), de taille définie, et qui permet d'identifier facilement les données initiales. Voir Annexe n°V.3.

Forge logicielle | Software Forge (conventionally referred to « code base repo » or « GitHub repo ») :

Une forge est une plateforme d'hébergement de projets logiciels, correspondant à un environnement web regroupant un ensemble d'outils qui permettent le développement collaboratif et distribué de logiciels. Elle offre un portail communautaire et l'accès à un site internet, un ensemble d'outils de gestion de projet et un environnement de développement collaboratif. Les services disponibles vont de la fourniture d'un système de gestion des versions à des trackers permettant de faire remonter des demandes de fonctionnalité, réaliser le suivi des bogues, de la gestion de tâches ; la livraison des paquets et fichiers ; une intégration continue ; la gestion de documents (wiki) ; et d'autres services (forums, listes de discussion, sondages, etc.).

Fork | Fork :

Peut-être traduit par *bifurcation*, mais, même en français, cet anglicisme s'est imposé. Suivant la situation, il peut qualifier un événement (volontaire ou non) qui voit un réseau* se scinder en deux ou plusieurs réseaux* (*Fork* de chaîne*), avec autant de registres* différents de transaction*. Il sert aussi généralement à qualifier les modifications protocolaires considérées comme importantes, pour les faire évoluer dans une direction souhaitée (ajout/suppression de fonctionnalités, changement d'architecture, etc.). On distingue alors les *Soft Forks** des *Hard Forks**, comme leur dimension plus ou moins contentieuse. Un Fork* de chaîne peut se produire suivant un bug logiciel, qui induit alors une perte de la *consistance** des *données endogènes** puisque des clients logiciels différents ne suivent plus les mêmes règles protocolaires ; ou quand une modification du protocole de registre* distribué est entreprise et non suivie par l'ensemble des acteurs, donnant lieu à un *Hard Fork** contentieux. Ces deux branches de programmes devenues non compatibles donnent naissance à deux protocoles de registre* distribué différents qui existent de manière autonome, le Fork* devenant un moyen politique d'émancipation et de recomposition d'acteurs autour de valeurs et d'intérêts différenciés.

Horodatage | Timestamp :

Processus d'enregistrement de la date et de l'heure exactes auxquelles un événement se produit. Il est couramment utilisé dans les fichiers journaux, les bases de données, les documents numériques et les systèmes de suivi pour assurer la traçabilité et l'intégrité des données.

Hors-protocole | Off chain :

Interactions, transactions*, processus qui se produisent en dehors des frontières formelles du protocole de registre* distribué.

Journal local | Journal :

Correspond à un ensemble d'enregistrements consignés localement dans un nœud, qui n'est pas nécessairement conforme au consensus des autres

nœuds*. Les Journaux locaux sont partiels, provisoires et hétérogènes.

Unité(s) de Compte Native(s) (UCN) | Native currency(ies) :

La/les unités de compte émises et administrées au sein du protocole et utilisées typiquement pour réguler la production d'enregistrement*, payer les frais de transaction* d'usage du réseau*, conduire la politique monétaire en vue d'aligner les intérêts des parties prenantes. Leurs formes scripturales suivent la logique et le(s) format(s) du protocole considéré.

Langage de programmation | Programing language :

Notation formelle utilisée pour définir des codes informatiques et les faire exécuter par un programme. Il comprend un ensemble d'instructions produisant divers types de résultats. La description d'un langage de programmation* se divise généralement en deux : la syntaxe (forme) et la sémantique (signification). Elles peuvent être définies par un document de spécification ou ne relever que d'une implémentation dominante traitée comme une référence. Les développeurs* peuvent utiliser de nombreux langages de programmation aux caractéristiques différentes pour réaliser des codes sources qui doivent encore être compilés pour être traduits en langage machine de bas de niveau. Ce langage machine, le langage natif d'un processeur, ne correspond qu'à des instructions codées en binaire. Par ex. : C++, Python, JavaScript, Solidity, Bytecode, etc.

Livre Blanc | White Paper (WP) :

Appellation qui tire son origine de la vie politique anglaise, où des documents imprimés sur un papier blanc servaient à présenter des politiques gouvernementales, et les soumettre à l'avis de la population. Ce terme a été utilisé par les entreprises pour décrire certains projets ou politiques commerciales. Désigne, dans notre champ, une publication plus ou moins longue, qui vise à donner une somme d'informations sur un projet donné. Le Livre Blanc sert à exposer un objectif comme les moyens proposés pour le résoudre. Publié par le/les instigateur(s) du projet, il peut aussi contenir des informations sur le financement du projet, un plan de route, un budget indicatif et une description de l'équipe qui travaille au développement. Un WP n'entre pas forcément profondément dans les détails techniques ; aussi, des Yellow Papers peuvent être publiés. Ces derniers correspondent à une version plus technique du WP, où sont présentés les détails technologiques, voire scientifiques, du projet.

Maximaliste (Bitcoiner) | Maximalist (Bitcoiner) :

Terme apparu en 2014, souvent attribué à Vitalik Buterin (2014a). Il désigne les *bitcoiners** pour qui Bitcoin devrait dominer toutes les autres CM (qualifiées d' « altcoins* » ou de « shitcoins »), considérées comme inférieures ou inutiles. Ils considèrent qu'un environnement d'une multiplicité de CM concurrentes n'est pas souhaitable et que toutes les innovations, le développement dans le domaine crypto devraient se faire exclusivement sur Bitcoin. Par extension, le terme *maximaliste* peut également désigner les fervents défenseurs d'une cryptomonnaie* spécifique et rejetant toutes les autres.

Monnaies digitales | Digital Money :

Catégorie générique recouvrant les monnaies basées sur une technologie de registre* distribué, mais ne se limitant pas aux cryptomonnaies* (CM). Elle englobe de nombreux objets relevant des logiques de signature ou de sceau, en fonction de l'existence d'acteurs centraux disposant de droits exorbitants sur le protocole, les données et le réseau*. On peut distinguer en son sein, en plus des CM, les unités de compte émises par des entités privées, comme Tether, qui sont des monnaies numériques privées, et des monnaies publiques, avec l'arrivée des monnaies digitales* de banque centrale (CBDC), dont la confiance repose sur une autorité émettrice publique. Voir encadré Chap.II.3.

Nœud | Node :

De manière générale, ce terme recouvre les acteurs non humains et leurs opérateurs humains participant du réseau*, communiquant avec leurs pairs en suivant les règles canoniques du protocole de registre* distribué considéré. Ils peuvent revêtir différentes formes et, suivant celles-ci, prendre part à tout ou partie des processus liés au traitement des transactions* et à la production d'enregistrements ou à leur vérification : nœuds* mineurs, nœuds* complets, etc.

Nonce | Nonce :

Correspond en cryptographie* à un nombre arbitraire (aléatoire ou pseudo-aléatoire) destiné à être utilisé une seule fois. Pour ce qui est des fonctions de *preuve de travail**, certains processus demandent de fournir un nonce qui, combiné au bloc de données mis en entrée d'une fonction de hachage*, fournit un résultat ayant certaines caractéristiques recherchées, rendant beaucoup plus difficile de créer un résultat cible que de le vérifier. Pour Bitcoin, c'est ce nonce qui est modifié par les opérateurs de transaction* à

chaque tentative de *preuve de travail**, jusqu'à l'obtention d'une *empreinte numérique** d'enregistrement inférieure ou égale à la *cible de difficulté**. Aussi, l'activité des opérateurs de transaction* est de trouver en premier le *nonce* qui, combiné aux données initiales de l'*enregistrement candidat**, permet d'obtenir une empreinte numérique* valide. Le *nonce* peut prendre un sens différent pour ce qui a trait à Ethereum, car, en plus du sens précédent, il correspond aussi à la numérotation des transactions* effectuées et traitées par un compte de portefeuille.

Passerelle | Gateway :

Contient l'ensemble des acteurs qui fournissent une interface entre le système de protocole de registre* distribué et le monde extérieur. On retrouve ici les bourses d'échange crypto fiat qui offrent une passerelle monétaire, mais aussi de nombreux autres services comme les explorateurs de registre*, par exemple.

Preuve de travail* | Proof of Work (PoW*) :

Correspond à un processus nécessitant de résoudre un défi cryptographique : obtenir une empreinte cryptographique d'un niveau de difficulté donné. Pour les protocoles de registre* dont le consensus repose sur une Proof of Work, ce processus est appelé « mining », et les opérateurs qui s'en chargent sont les « mineurs ».

Portefeuille | Wallet :

Correspond à un logiciel client capable de générer, stocker et administrer des couples de clefs cryptographiques afin de conserver et transférer ses CM et actifs digitaux.

Protocole informatique | Protocol :

Ensemble de règles et de procédures standardisées permettant à des machines en réseau* de communiquer entre elles. Il détermine, pour un système donné, les modalités de son fonctionnement.

Problème de double dépense | Double spending problem :

Problème auquel fait face toute monnaie numérique. Il correspond à un acte frauduleux par lequel une unité de compte, du fait de son caractère numérique, est falsifiable et duplicable, et peut être dépensé plus d'une fois. Comme pour la fausse monnaie, une telle pratique peut faire augmenter la masse monétaire et éroder la confiance des utilisateurs dans le système de paiement.

Récompense d'enregistrement | Block reward :

Correspond à une récompense en *unité de compte native** perçue par un opérateur de transaction* dont l'*enregistrement candidat** devient canonique en étant intégré au *registre**. Elle tient le rôle de création monétaire, rémunérant les acteurs en contrepartie du travail de traitement et de sécurisation des transactions* et du *registre*.

Registre | Ledger :

Correspond, à tout moment, à l'ensemble des enregistrements faisant autorité, consignés dans une portion substantielle des nœuds* participant au réseau*. Un *registre* se compose d'une série de différents enregistrements stockant des informations relatives aux transactions* qui ont lieu sur le réseau*. Les enregistrements intégrés dans un tel registre sont peu susceptibles d'être effacés ou modifiés, et sont considérés comme finaux. Voir *finalité de paiement**.

Réorganisation d'enregistrement | Record reorganisation :

Il s'agit d'un événement normal de tout protocole de registre* distribué où un nœud du réseau* découvre qu'un autre enregistrement valide existe en parallèle de celui qu'il suit. Par l'algorithme de consensus et à la suite d'un nouveau cycle de production d'enregistrement, cette version alternative du registre* est devenue canonique pour tous, excluant un ou plusieurs enregistrement(s) auparavant inclus, dit(s) « orphelin(s) ». L'attaque 51% dont parle extensivement Nakamoto se rapporte à un cas critique de ce phénomène où une entité disposant de plus de 51% de la puissance de calcul va pouvoir préparer en secret un historique concurrent valide et plus lourd que celui actuellement considéré comme canonique, afin de tirer profit de l'annulation de transactions* effectuées au sein de l'historique rendu orphelin. Voir Annexe n°V.5.

Réseau* | Network :

Correspond à l'ensemble des acteurs - humains ou non - et des processus interconnectés qui mettent en œuvre un protocole de communication entre différentes machines ou *nœuds** leur permettant d'échanger des informations. Les réseaux les plus répandus fonctionnent sur le mode de communication dit « client/serveur », où un ordinateur et son utilisateur - le client - demandent des informations par l'émission d'une requête à un serveur central qui en dispose et lui transmet en retour. C'est le cas des navigateurs et d'une grande majorité de sites Internet, par exemple. D'autres formes existent comme les *réseaux* pair-à-pair**.

Réseau pair-à-pair | Peer-to-peer Network :

Correspond à un réseau* où les nœuds* qui participent à l'échange d'information sont, contrairement au mode « client/serveur », tour à tour client et serveur, demandeur et donneur. Chaque nœud* est sur un pied d'égalité avec les autres nœuds* constituant le réseau*, et ils sont donc des pairs. Il n'y a plus un acteur qui dispose des informations auxquelles souhaite accéder une multitude d'utilisateurs, car les informations sont répliquées sur une multitude de nœuds*.

Résistance à la censure | Censorship Resistance :

Correspond à l'impossibilité pour un acteur ou un cartel d'effectuer unilatéralement et arbitrairement : (i) une modification des règles du protocole ; (ii) de bloquer ou de censurer des transactions* ; et (iii) de saisir un compte ou de geler des avoirs.

Script à exécution programmatique | Programmatically-executed scrypt :

Script informatique qui, lorsqu'il est déclenché par un message particulier, est exécuté par le protocole de registre* distribué. Lorsque le code est capable de fonctionner suivant les attentes des parties engagées, le caractère déterministe de l'exécution réduit le niveau de confiance nécessaire aux participants individuels dans leurs interactions réciproques. Ils sont communément appelés « Smart contracts* » en raison de la capacité des scripts à remplacer certaines relations contractuelles ou fiduciaires, comme la conservation ou le séquestre, par du code. En revanche, ils ne sont ni autonomes, ni adaptatifs (« intelligents »), et encore moins un contrat au sens juridique du terme.

Signature cryptographique | Cryptographic signature :

Reposant sur la cryptographie* asymétrique, ce type de signature permet de vérifier mathématiquement la possession d'un ensemble de données, si tant est que l'utilisateur conserve secrète sa clef privée pour signer ses transactions*. Voir Annexe n°V.1.

Sortie de transaction non dépensée | UTXO :

Forme prise par les unités de compte reçues mais non encore dépensées pour les systèmes de protocole de registre* distribué qui, comme Bitcoin, fonctionnent sur ce type d'architecture : ici, l'état de la structure des *données endogènes**, contenues dans le *registre** à un instant T, représente la collection de toutes les UTXO* existantes. Ainsi, une transaction* correspond à une cession authentifiée d'une ou plusieurs UTXO* (qui sont à l'*output* de la transaction*) et qui donnera lieu, en sortie, à une UTXO* reçue par le receveur (pour lui en *input*). D'autres architectures peuvent être choisies quant au suivi de l'état de la structure de donnée, comme avec Ethereum et son *modèle basé sur compte**.

Modèle basé sur compte | Account based Model :

Le modèle basé sur compte, comme pour le modèle basé sur UTXO*, sert en premier lieu au suivi de l'état de la structure de donnée. Mais ici, comme pour un compte bancaire traditionnel, à un instant T, le système de protocole de registre* distribué renseigne des soldes pour chaque compte. Une transaction* authentifiée correspond alors à une cession qui réduit le solde de l'envoyeur d'autant que ce que le receveur reçoit sur son compte. Ce choix d'Ethereum s'explique par le fait que, en plus des comptes personnels - ou comptes de détenteur externe ou EOA - contrôlés par une clé privée, il existe des comptes contrôlés par une commande/code de contrat (les smart contracts*, SC). Le modèle basé sur compte répond alors à des besoins spécifiques et permet d'augmenter la capacité d'exécution des smart contracts* du protocole de registre* distribué qui fait ce choix (plus grande simplicité, gain de place, fongibilité accrue).

Système de protocole de registre distribué | DLT system :

Système d'enregistrement électronique qui permet à un réseau* de participants indépendants d'établir un consensus autour d'un ordonnancement de transactions* validées cryptographiquement qui fait autorité. Les enregistrements sont rendus persistants par fait de réplication des données sur une multitude de nœuds*, et sont témoins de violabilité /d'intégrité (temper-evident) par les liens cryptographiques qui les relient (les hash*). Le résultat partagé du processus de réconciliation/consensus constitue un registre* transactionnel canonique faisant autorité.

Système de protocole de registre fermé (ou avec autorisation) | Permissioned System :

Protocole de registre* distribué de type « Classique », car premier à avoir été développé. Ce système correspond à la définition générale des DLT ; l'archivage partagé* n'est pas ouvert à tous et seuls les participants formellement reconnus et autorisés peuvent participer. Cette sélection est effectuée par l'/les autorité(s) compétente(s) – entité(s) qui conçoi(ven)t et déploi(en)t le système – et inscrite dans le code logiciel fourni par les administrateurs.

Système de protocole de registre ouvert (ou sans autorisation) | Permissionless System :

Protocole de registre* distribué qui sous-tend ce que nous considérons et qualifions de CM. Dans ce type de système, l'archivage partagé* est ouvert à tous sans qu'une entité ou un groupe ne se voie reconnaître protocolairement de privilège quelconque.

Temps d'enregistrement | Block time :

Le temps d'enregistrement ou de bloc fait référence au temps moyen nécessaire pour créer (ou miner) un nouveau bloc sur la blockchain et conclure un cycle de traitement des transactions*. Pour Bitcoin, le temps d'enregistrement moyen est d'environ 10 minutes.

Tolérance à la partition | Partitioning Tolerance :

Correspond à une propriété recherchée par tout système informatique de calcul distribué permettant qu'aucune défaillance - à l'exception d'une panne totale du réseau* - d'un ou plusieurs nœud(s) n'empêche le système de répondre correctement.

Traitement des transactions | Transaction processing :

Correspond à l'ensemble des processus qui spécifient les mécanismes de mise à jour du registre. Il définit : (i) quels participants ont le droit de mettre à jour l'ensemble d'enregistrements partagés faisant autorité (sans autorisation pour les systèmes ouverts et avec autorisation formelle pour les systèmes privés ou de consortium), et (ii) comment les participants parviennent à un accord consensuel sur la mise en place de cette mise à jour. Appelé aussi « mining ».

Transaction | Transaction :

Renvoie à toute modification proposée au registre ; elle n'est pas nécessairement de nature économique (transfert de valeur). Une transaction* peut être soit non confirmée (non incluse dans le registre, elle se trouve encore seulement dans la mempool), soit confirmée (incluse dans le registre). Une même transaction* peut contenir une multitude de transactions* différentes : différents receveurs ; différentes modifications de registre, etc.

Validation | Validation :

Correspond à l'ensemble des processus requis afin d'assurer que les acteurs arrivent indépendamment à la même conclusion en ce qui concerne l'état du registre. Cela inclut la vérification de la validité des transactions* non confirmées, la vérification des enregistrements, qu'ils soient confirmés ou non, et l'audit de l'état du système.

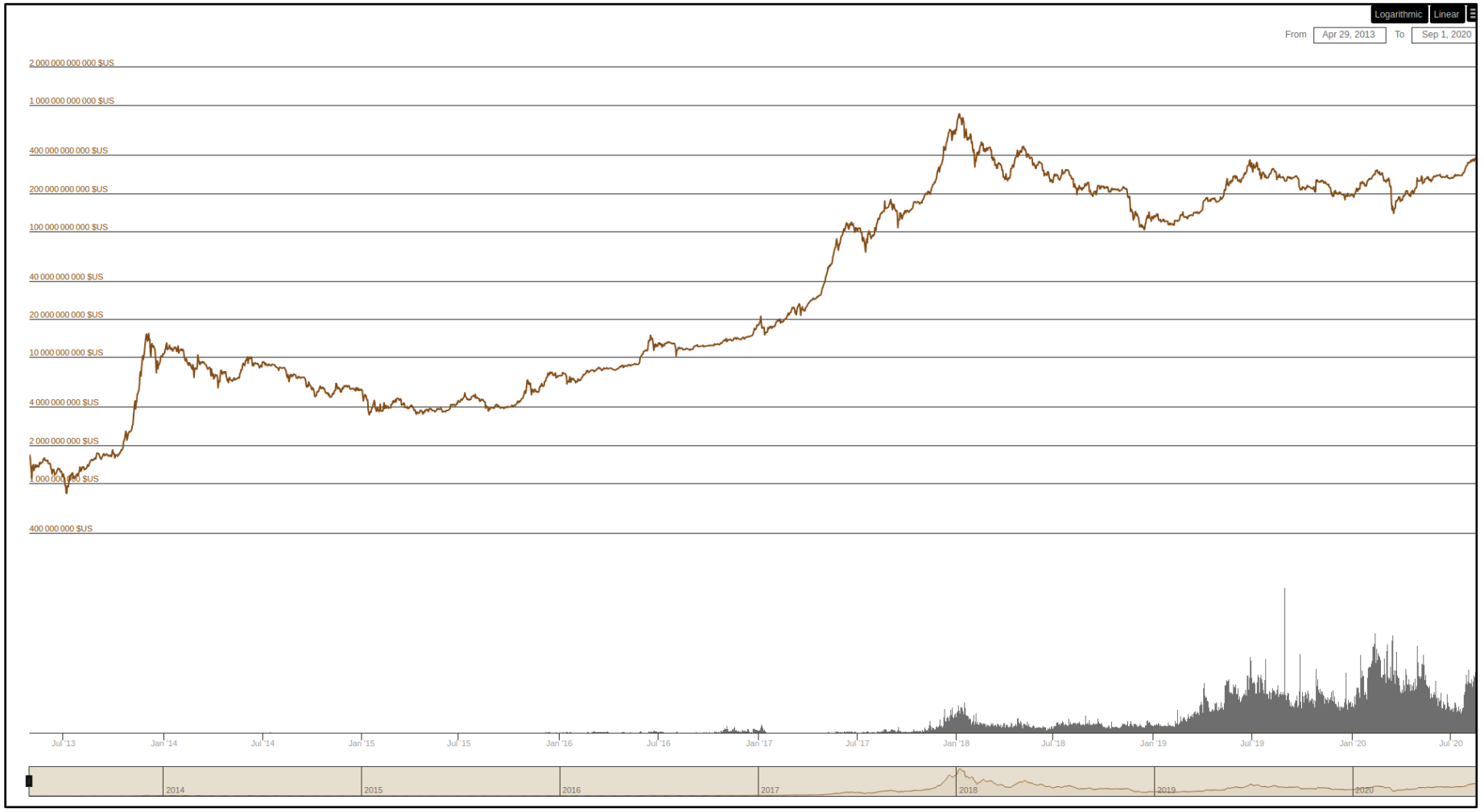
Validation indépendante | Independent Validation :

Désigne la capacité du système de protocole de registre* distribué à permettre à chaque participant la vérification indépendante de l'état des transactions* et de l'intégrité du système.

ANNEXES

Annexe I : Données synthétiques relatives à l'écosystème des CM pris dans son ensemble

Annexe I.1 : Capitalisation totale et taux de dominance sur le marché des crypto-actifs (~5868 actifs listés sur Coingecko), au 01/09/2020



Source : https://www.coingecko.com/fr

Source : https://www.coingecko.com/fr

Annexe I.2 : Capitalisation totale et taux de dominance de marché des crypto-actifs (~5868 actifs listés), au 01/09/2020

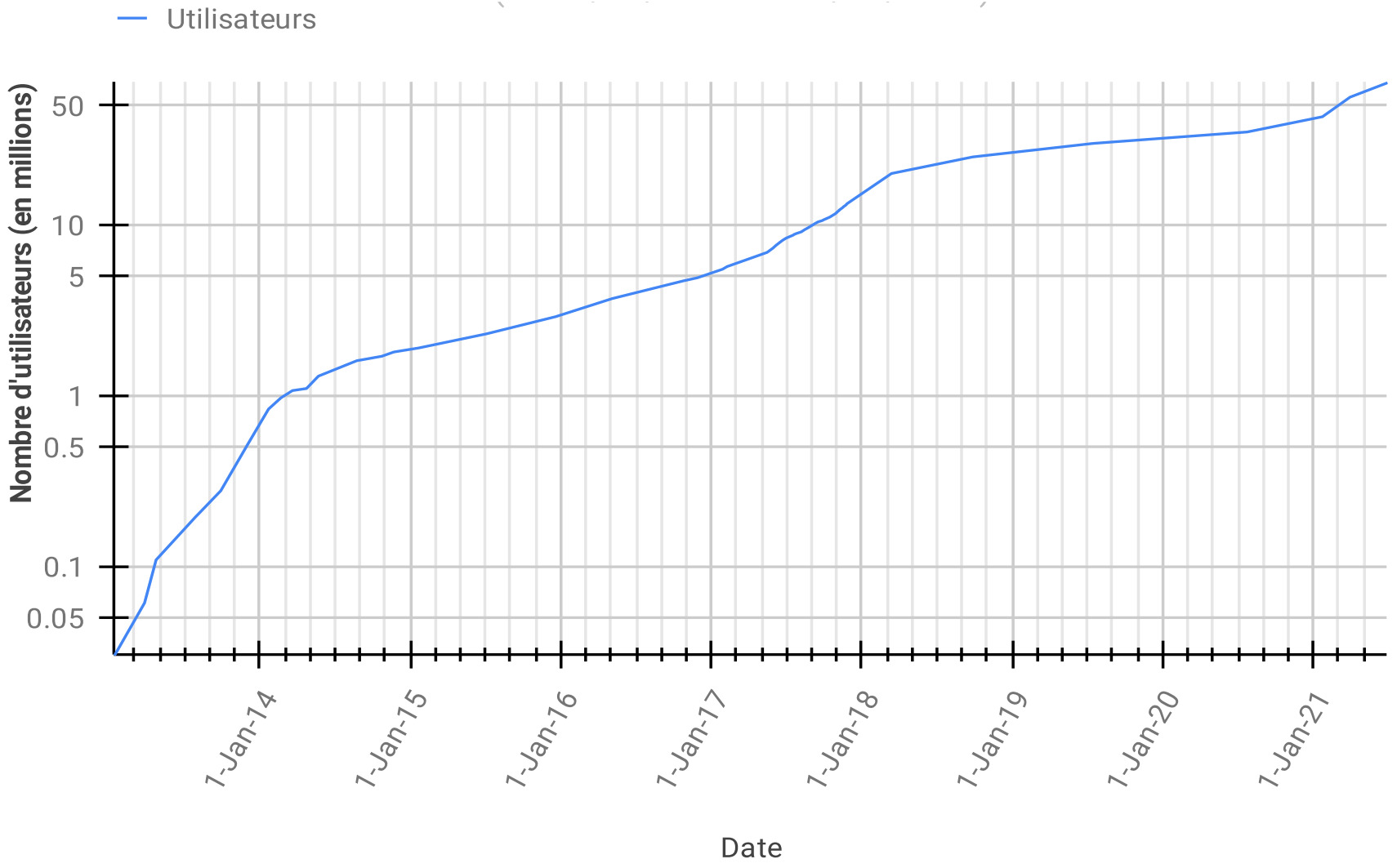
Rang	CM ou crypto-actif	Ticker	Cours ($)	Volume 24h (en $)	Capitalisation totale (en $)	Dominance (en %)
1	Bitcoin	BTC	11 909,63	23 529 258 593	220 049 317 281	54,89 %
2	Ethereum	ETH	460,92	17 249 915 593	51 787 809 789	12,91 %
3	Tether	USDT	1	39 137 093 048	13 442 100 350	3,35 %
4	XRP	XRP	0,29	1 906 782 832	13 155 811 083	3,28 %
5	ChainLink	LINK	16,21	1 099 639 778	6 240 933 623	1,55 %
6	Polkadot	DOT	6,72	555 583 850	6 092 040 460	1,51 %
7	Bitcoin Cash	BCH	280,63	2 493 105 816	5 198 817 899	1,29 %
8	Litecoin	LTC	62,75	2 472 163 202	4 102 489 879	1,02 %

9	Cardano	**ADA**	**0,1242**	**528 551 176**	**3 867 875 994**	**0,96 %**
10	Bitcoin SV	**BSV**	**199,14**	**758 820 514**	**3 688 194 961**	**0,92 %**
25 premières					**357 540 681 324**	**89,19 %**
50 premières					**374 229 952 997**	**93,35 %**
Effectif Total (5868 crypto-actifs*)				**94 529 688 590**	**400 851 587 974**	**100%**

Source : https://www.coingecko.com/fr, traitement de l'auteur.

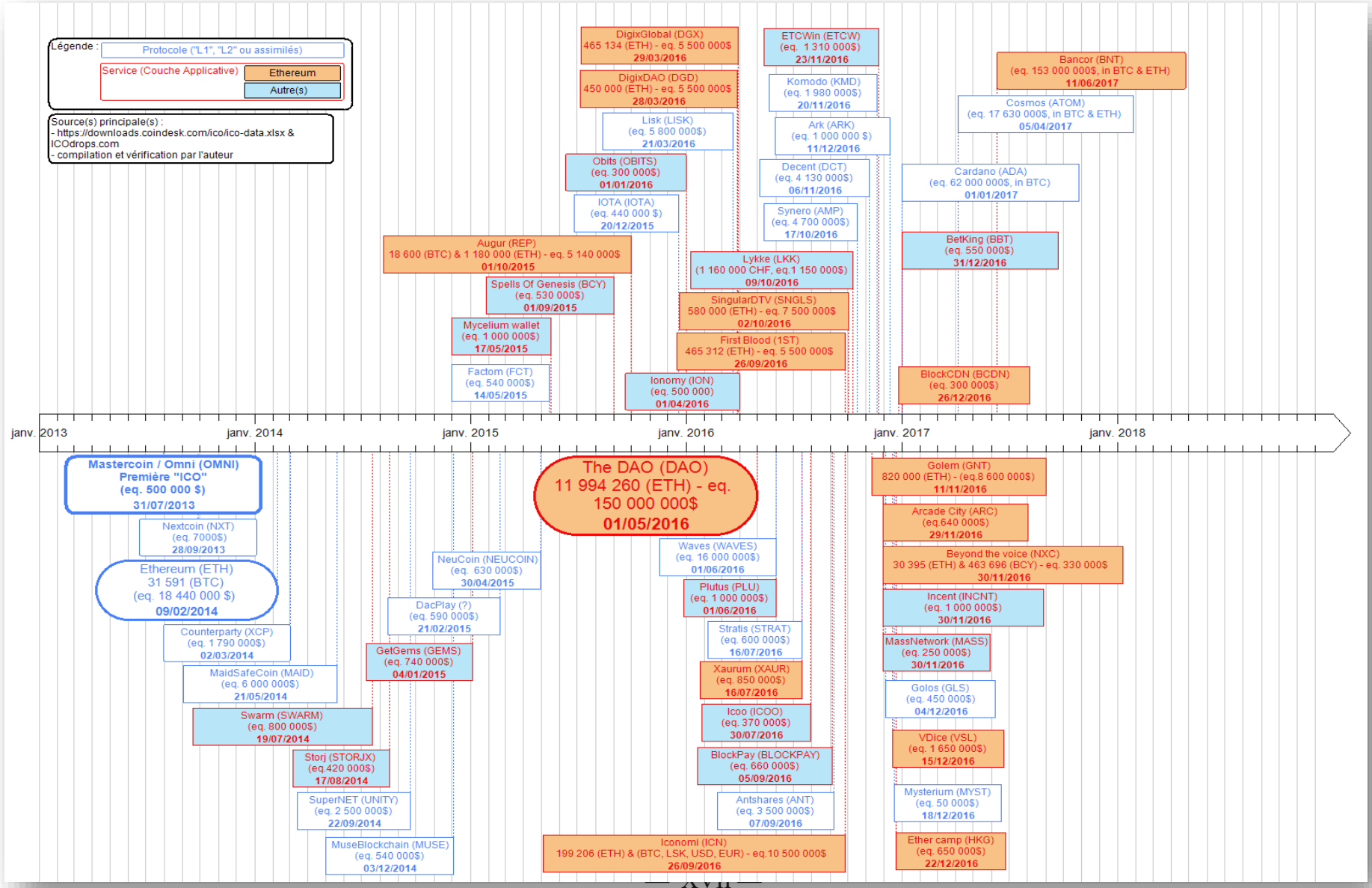
Annexe I.3 : Évolution du nombre d'utilisateurs de la plateforme Coinbase

(Du 13/01/2013 au 30/06/2021)



Source des données : Coinbase & @Alistairmilne

Annexe I.4 : Chronologies circonstanciées du phénomène des Initial Coin Offering (ICO), de juillet 2013 à juin 2017

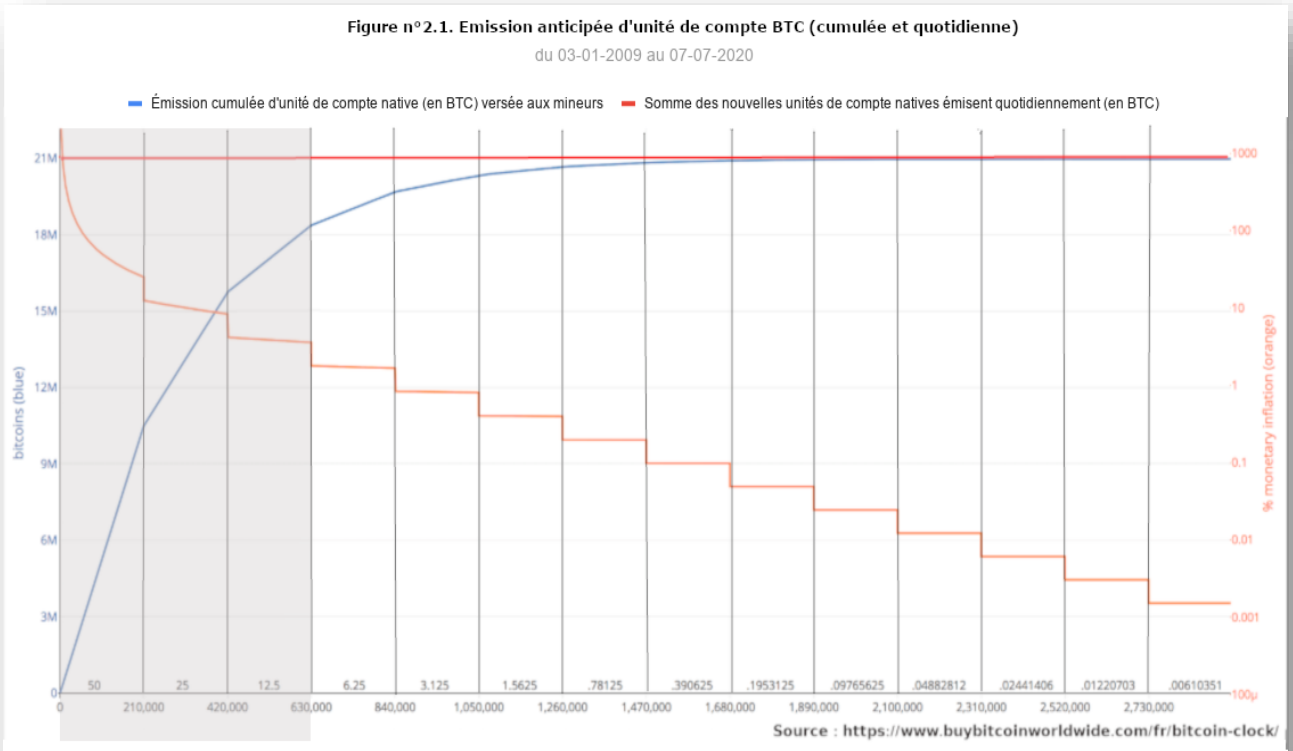


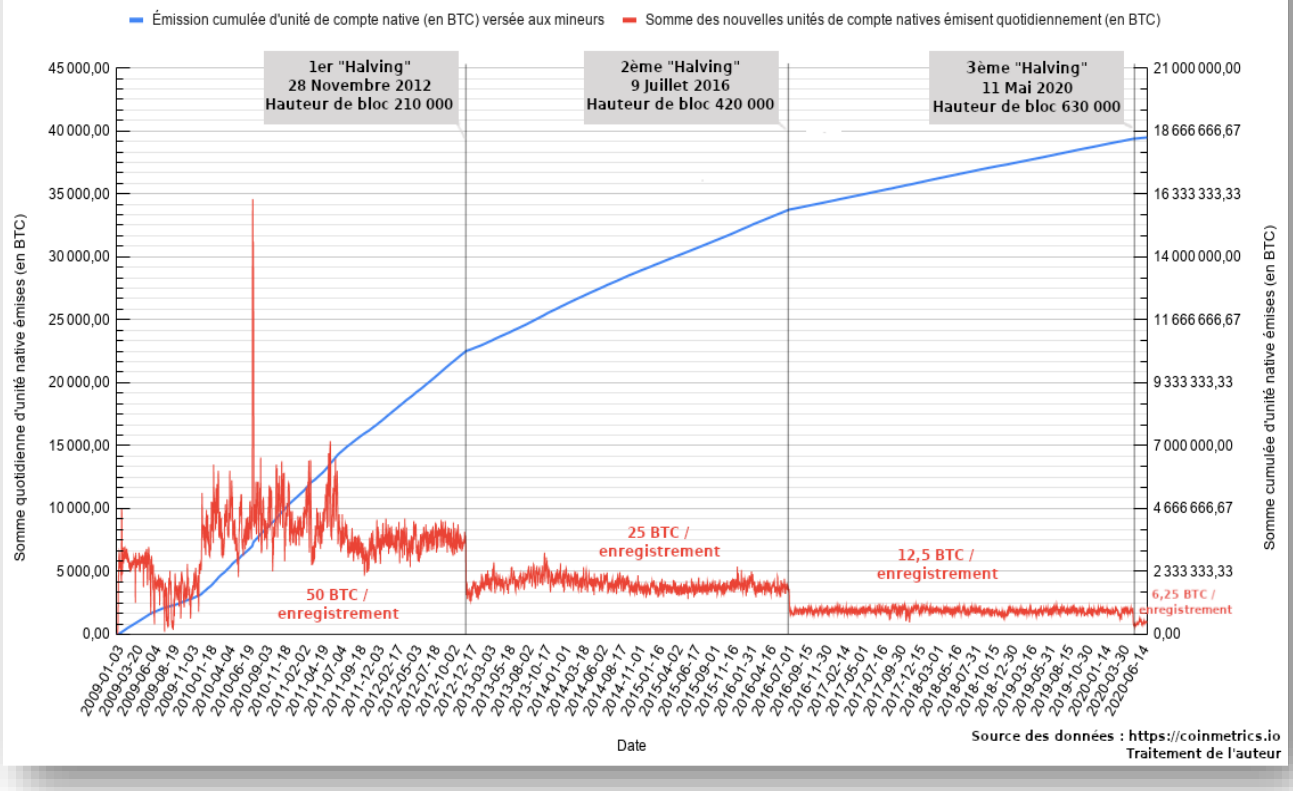
Annexe II : Données synthétiques relatives à l'écosystème de Bitcoin

Annexe II.1 : L'UCN bitcoin et sa décimalisation (matérielle et symbolique)

<table>
<tr><th colspan="3">Bitcoin et son UCN* bitcoin</th></tr>
<tr><td>Représentation symbolique des UCN*</td><td colspan="2"> 
</td></tr>
<tr><td>« Ticker » boursier & symbole</td><td colspan="2">BTC (ou XBT)
฿</td></tr>
<tr><td rowspan="7">Décomposition fractionnaire des UCN* et leur valeur de conversion en UCN* principale</td><td>Unité(s) fractionnaire(s) conventionnelle(s)</td><td>Valeur en UCN* (BTC)</td></tr>
<tr><td>Le « bitcoin » (ou BTC)</td><td>1</td></tr>
<tr><td>Le « Cent-bitcoin » | le « cBTC » | ou le « bitcent »</td><td>0.01</td></tr>
<tr><td>Le « Milli-Bitcoin » | le « mBTC » | ou le « millibit »</td><td>0.001</td></tr>
<tr><td>Le « Micro-Bitcoin » | le « µBTC » | ou le « bit »</td><td>0.000001</td></tr>
<tr><td>Le « Finney »</td><td>0.0000001</td></tr>
<tr><td>Le « Satochi »</td><td>0.00000001</td></tr>
<tr><td>Source :</td><td colspan="2">https://atozmarkets.com/news/simple-guide-to-bitcoin-units-of-measurement/</td></tr>
</table>

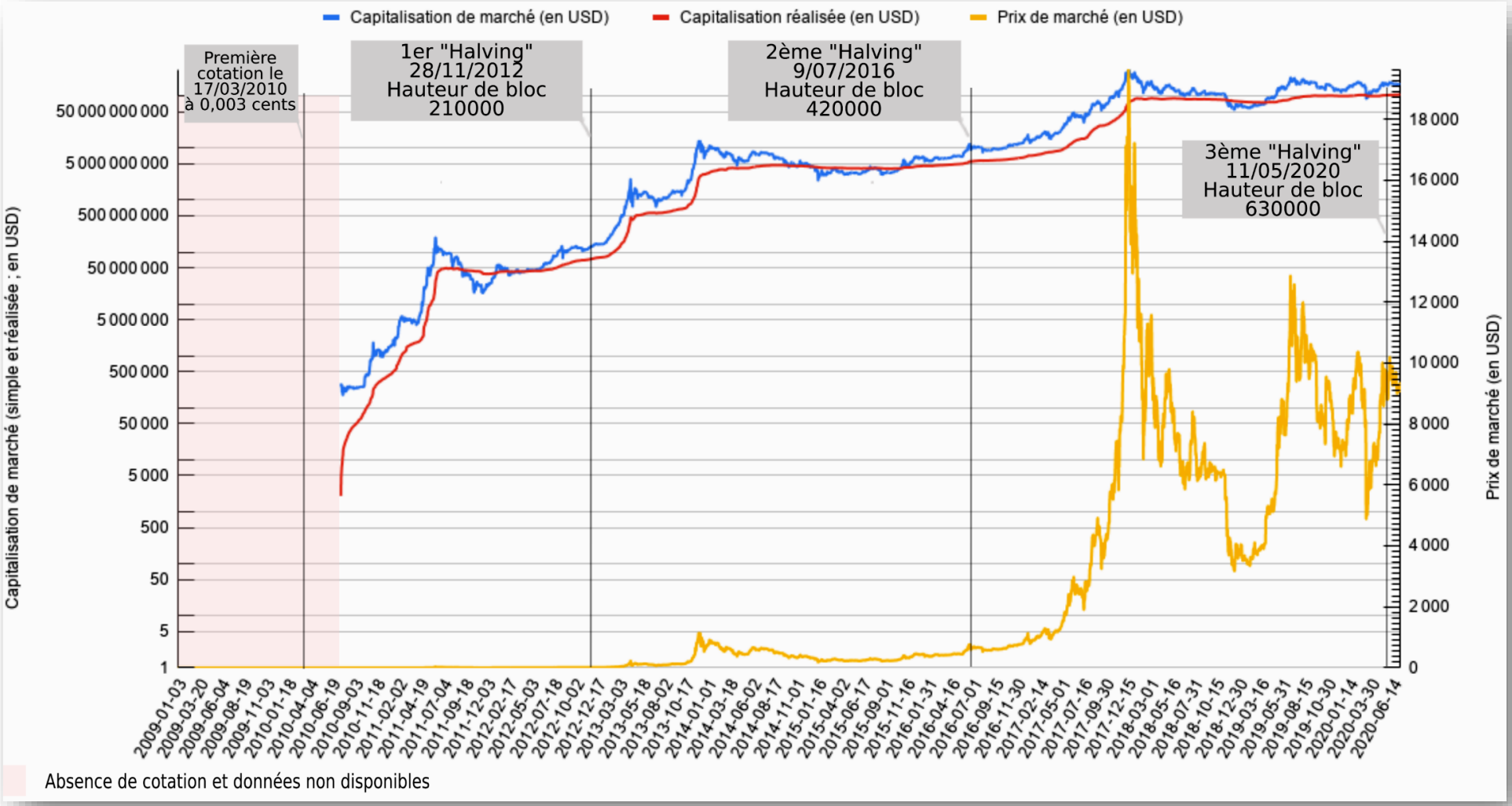
Annexe II.2 : Une offre monétaire programmatique : entre émission anticipée et effective





Annexe II.3 : Capitalisation de marché du BTC, en prix de marché [1] et réalisée [2], en USD

(du 18 Juillet 2010 au 07 Juillet 2020)



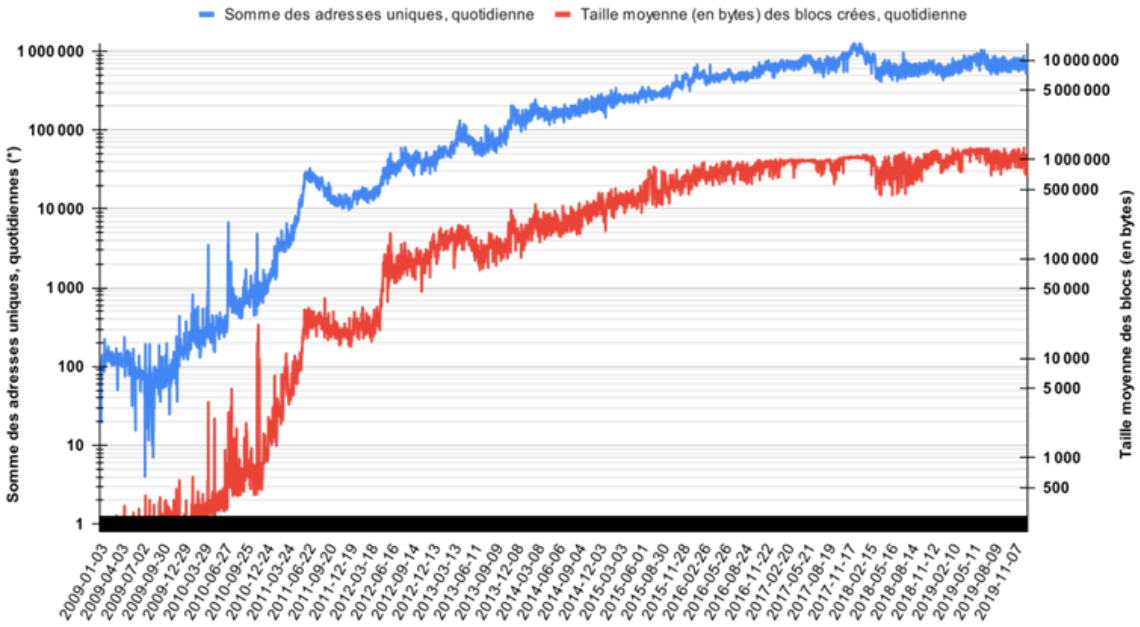
Source des données : https://www.coinmetrics.io; (*cf.* Chapitre 1 pour la 1ère cotation) ; traitement de l'auteur.

[1] Valeur agrégée en USD de l'offre actuelle, également appelée valeur du réseau ou capitalisation du marché.

[2] Valeur agrégée en USD basée sur le prix de clôture du BTC le jour de la dernière transaction impliquant chacune d'elles (leurs UTXO) : cette mesure est plus précise en ce qu'elle tient

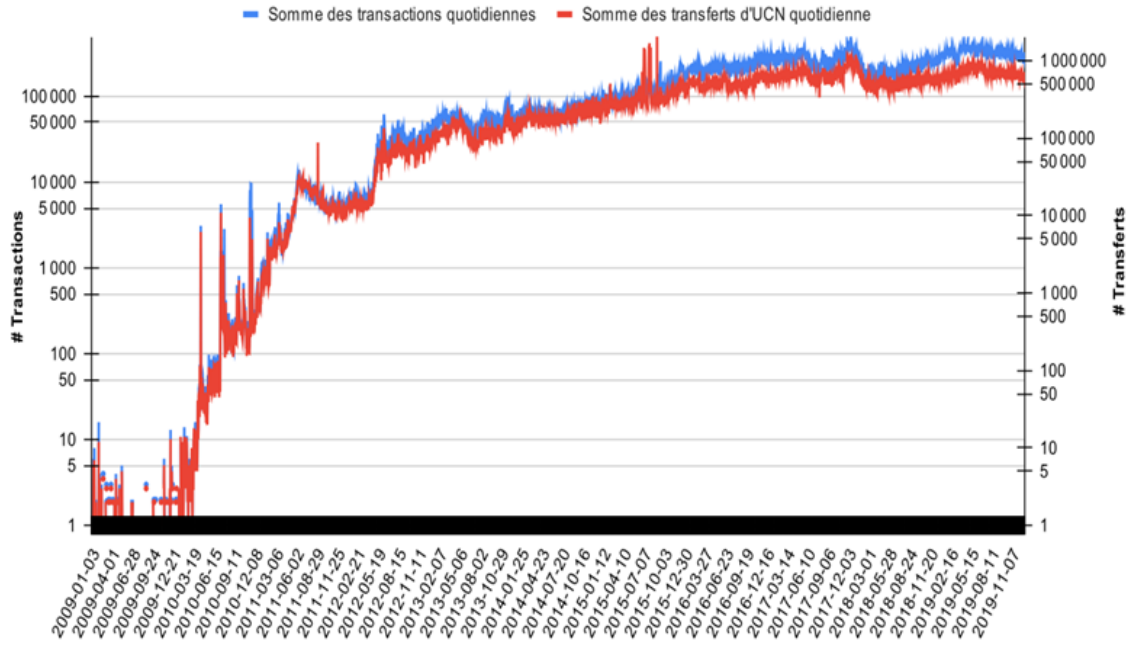
Annexe II.4 : Nombre d'adresses actives [1] et taille moyenne des enregistrements (en bytes), quotidien

(de janvier 2009 à décembre 2019, échelle logarithmique)



Annexe II.5 : Nombre de transactions [2] et transferts [3] quotidiens

(de janvier 2009 à décembre 2019, échelle logarithmique)



Source des données : https://www.coinmetrics.io; traitement de l'auteur.

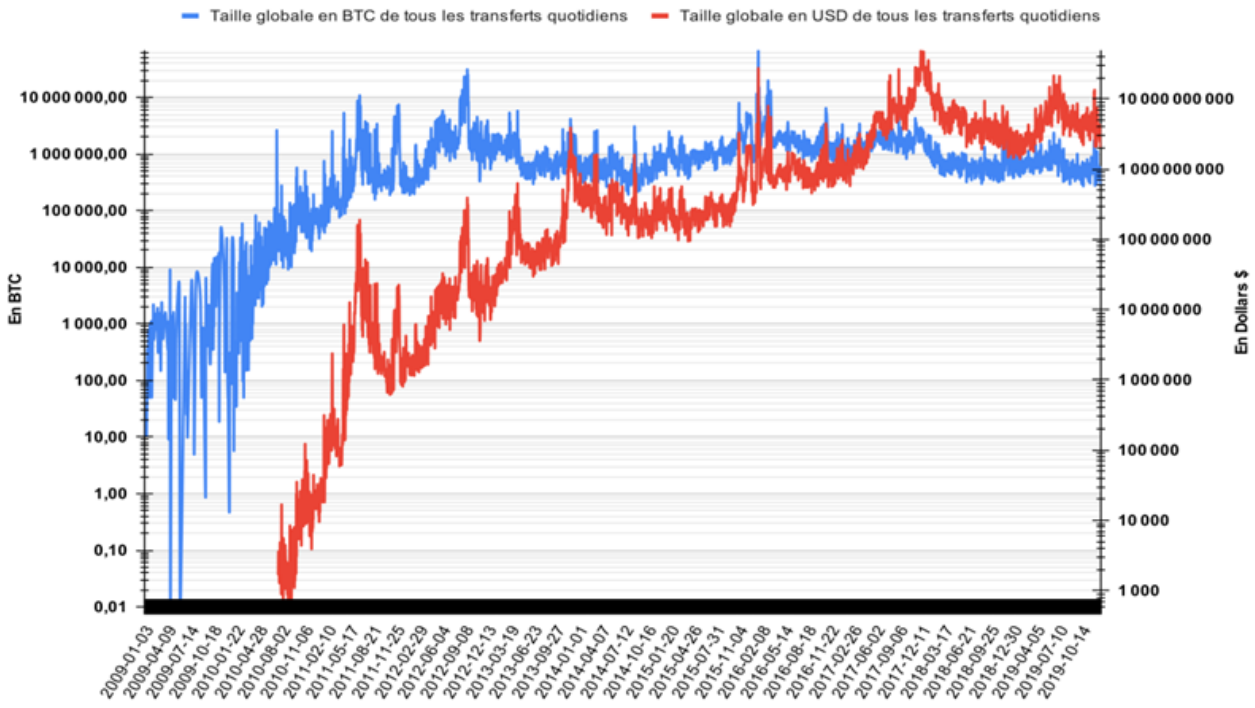
[1] Somme des adresses uniques actives quotidiennes (destinataires et envoyeurs, chaque adresse n'est comptée qu'une fois).

[2] Somme des transactions quotidiennes (exécutées ou non et avec transfert d'UCN ou non), hors transactions protocolaires (cf. *coinbase transaction*).

[3] Somme des transferts quotidiens : mouvements d'UCN d'une adresse à une autre, résultants d'une transaction et qui ont une valeur positive.

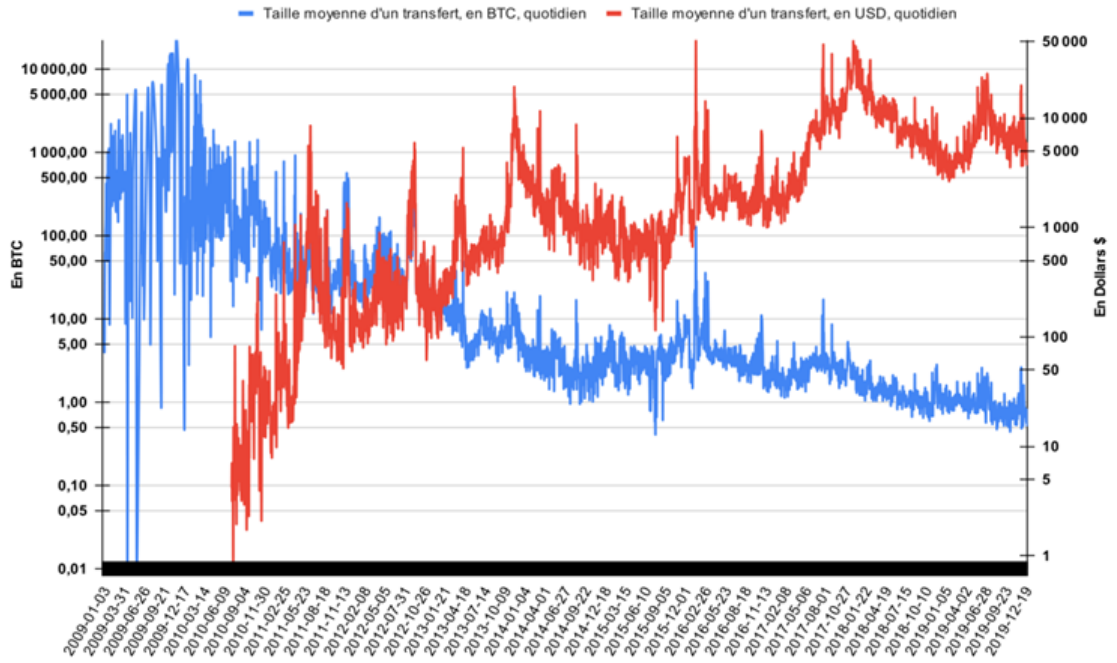
Annexe II.6 : Taille globale de tous les transferts quotidiens, BTC et USD[(1)]

(de janvier 2009 à décembre 2019, échelle logarithmique)



Annexe II.7 : Taille moyenne des transferts, en BTC et USD, quotidien[(2)]

(de janvier 2009 à mars 2019, échelle logarithmique)



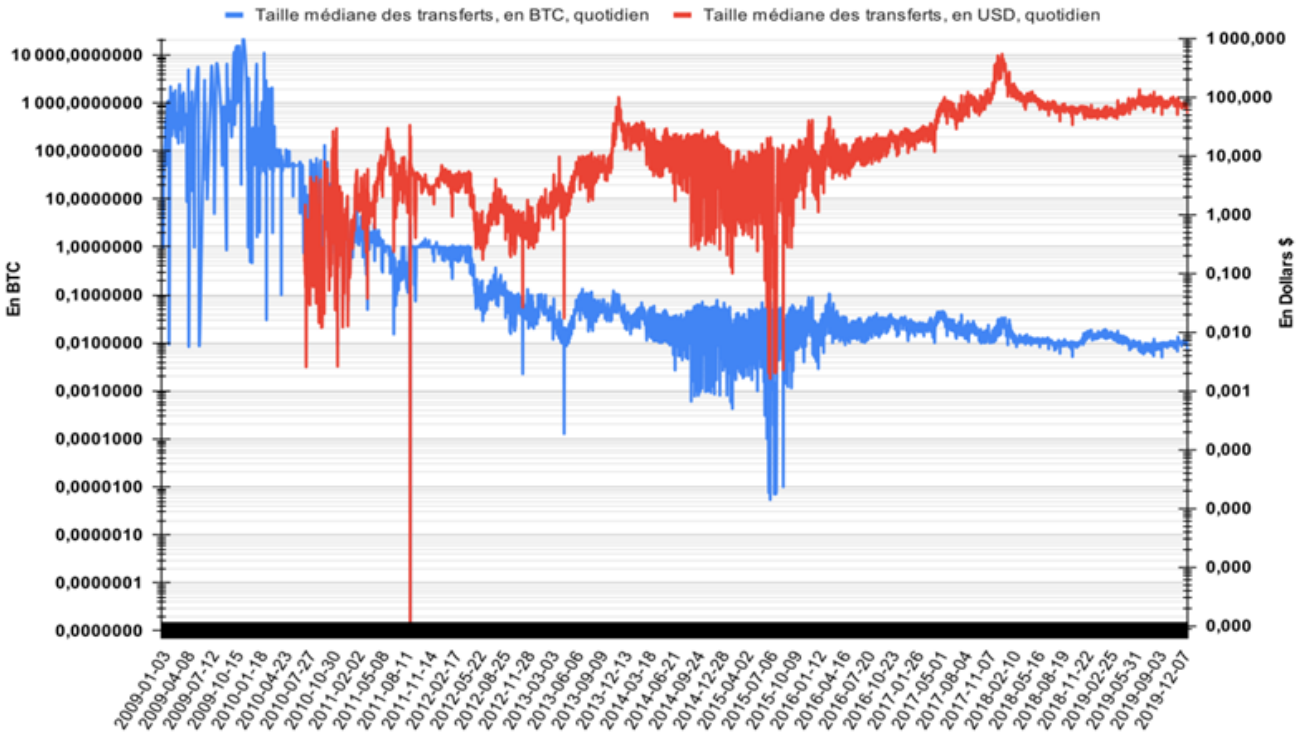
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

(1) Quantité totale d'UCN transférées (en BTC) et valeur agrégée des transferts (en USD), quotidienne.

(2) Quantité moyenne d'UCN transférée (en BTC) et valeur moyenne des transferts (en USD), quotidienne.

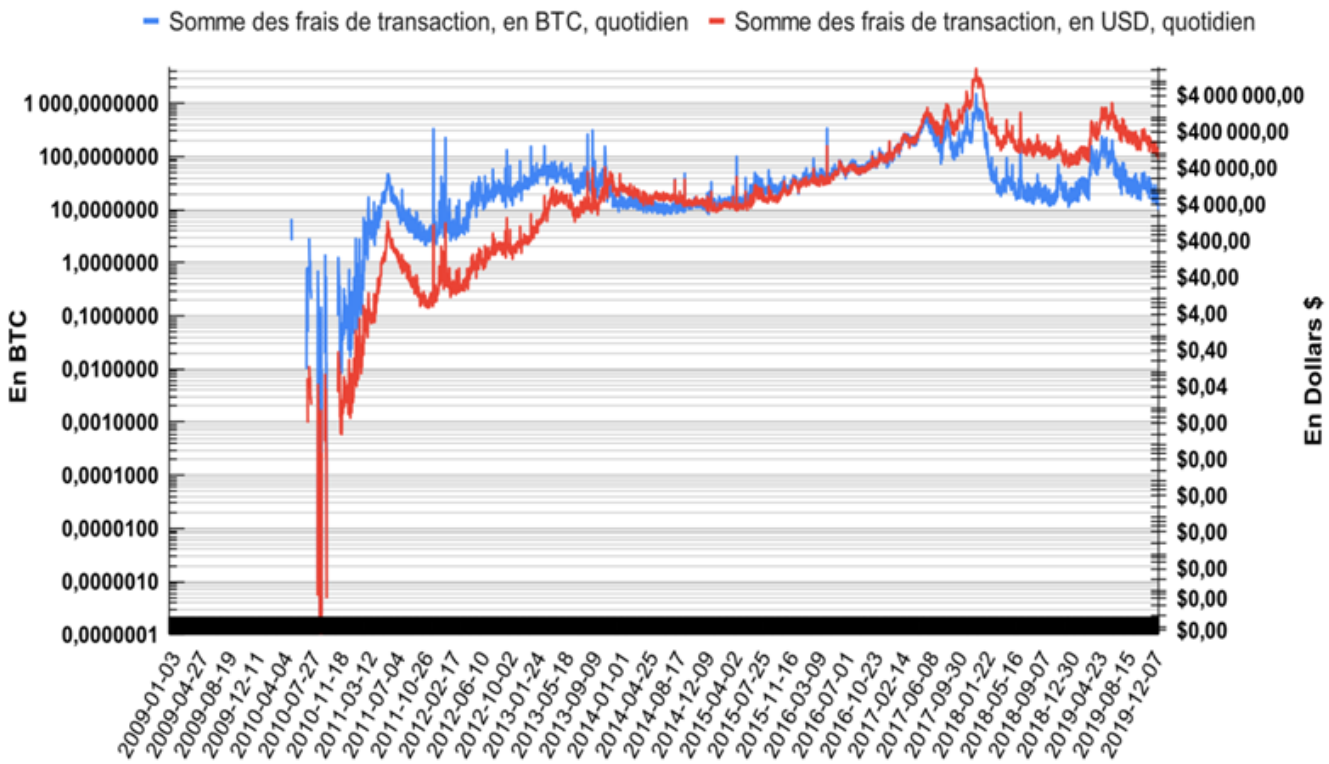
Annexe II.8 : Taille médiane des transferts, en BTC et USD, quotidien[1]

(de janvier 2009 à mars 2019, échelle logarithmique)



Annexe II.9 : Somme des frais de transaction, en BTC et USD, quotidien[2]

(de janvier 2009 à décembre 2019, échelle logarithmique)



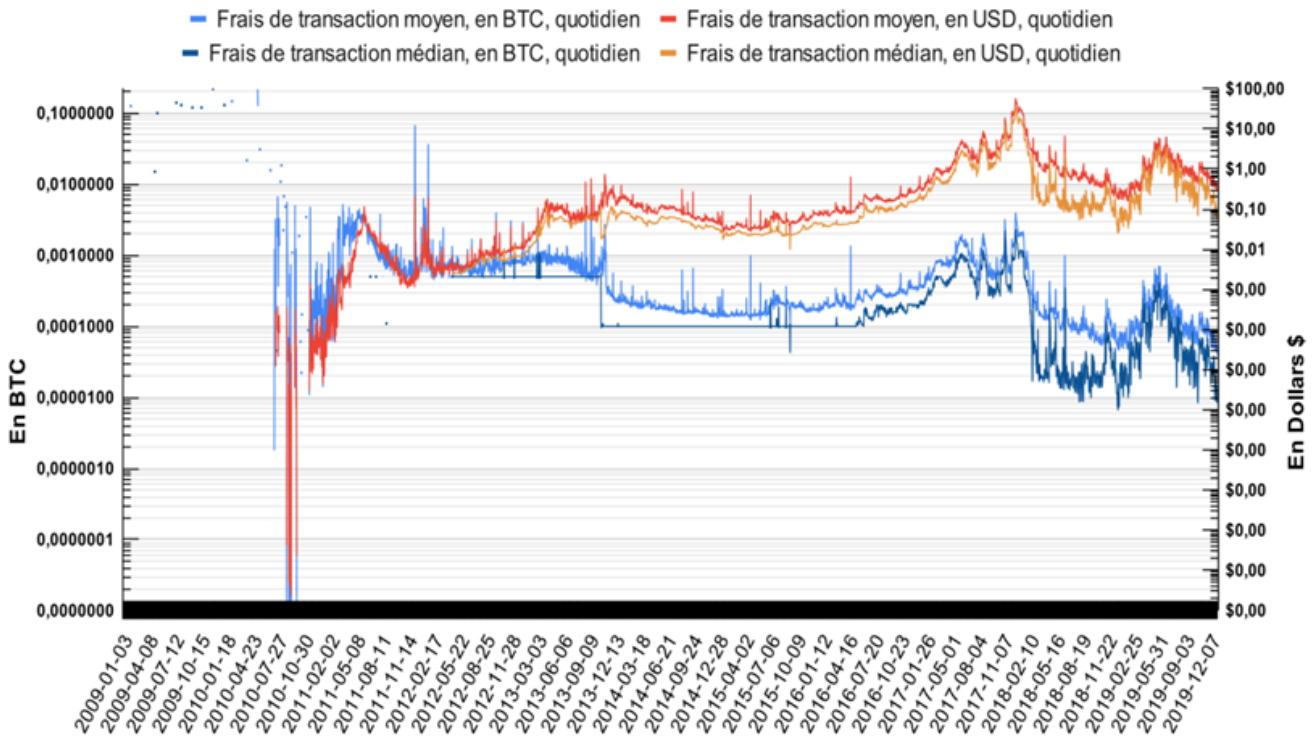
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

[1] Quantité médiane d'UCN transférée (en BTC) et valeur médiane des transferts (en USD), quotidienne.

[2] Somme des frais de transaction reçus par les mineurs, en BTC et USD, quotidien (hors récompenses d'émission monétaire).

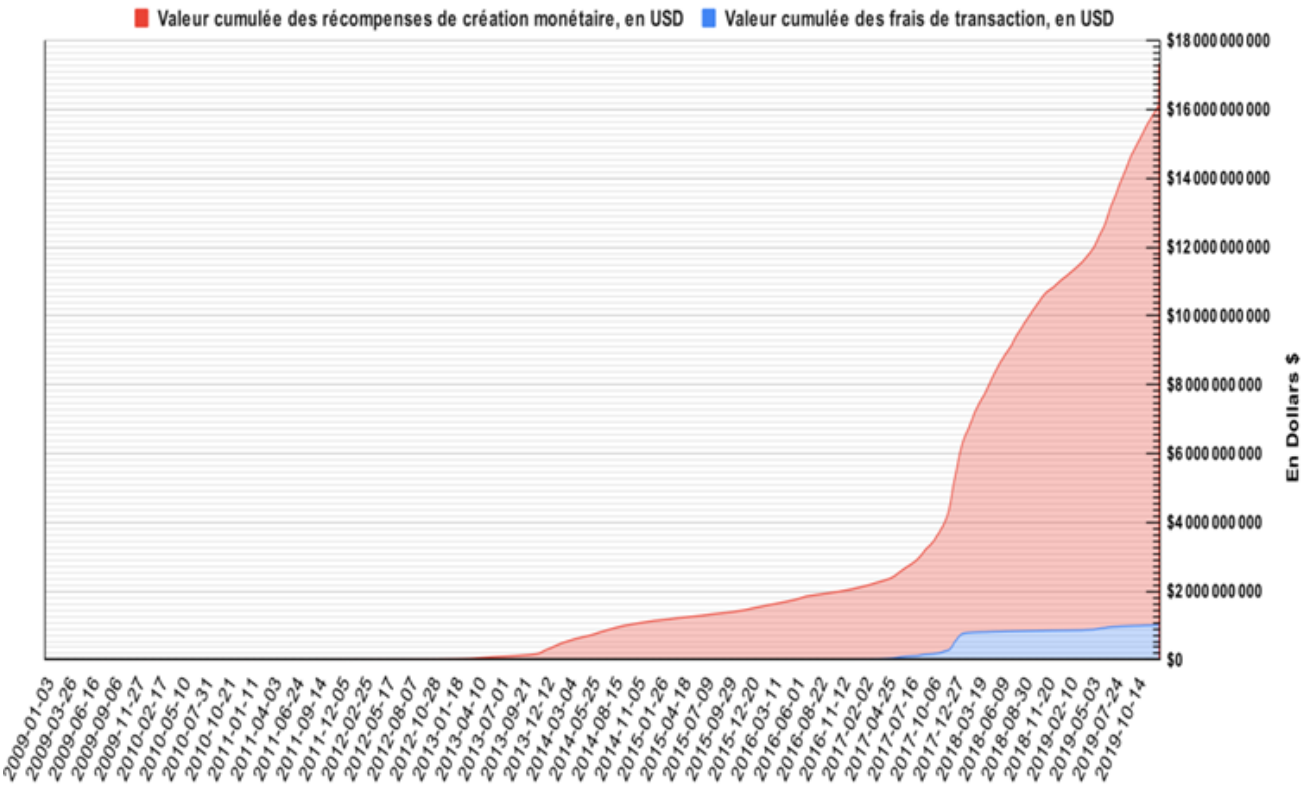
Annexe II.10 : Frais de transaction, moyen et médian, en BTC et USD, quotidien[1]

(de janvier 2009 à décembre 2019, échelle logarithmique)



Annexe II.11 : Revenu cumulé des « mineurs » en USD[2]

(de janvier 2009 à décembre 2019)



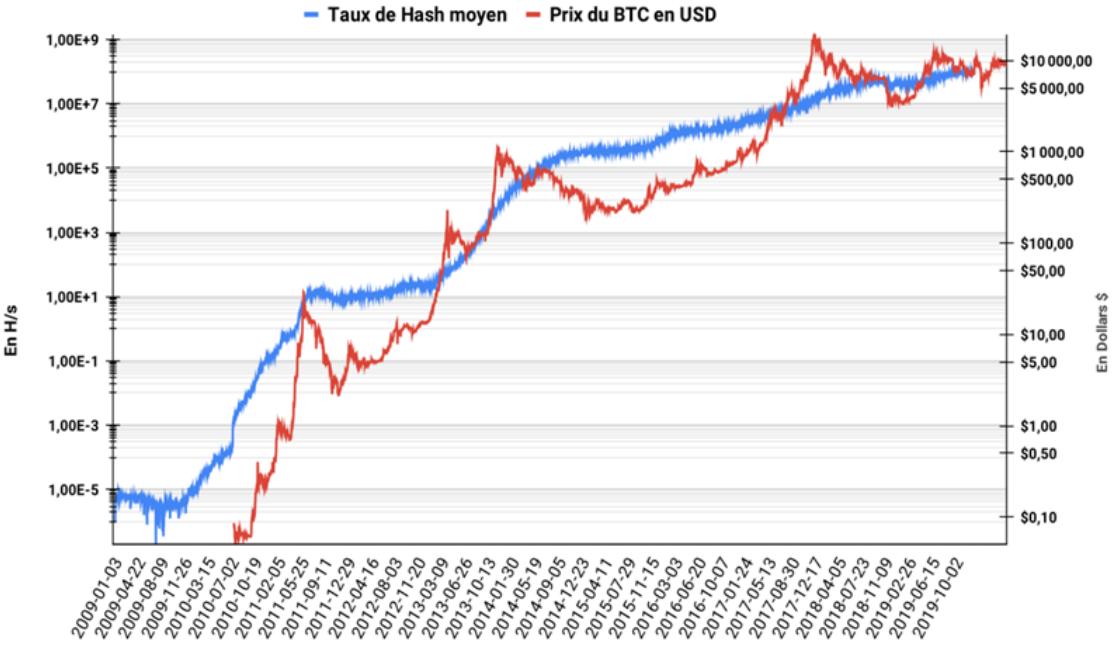
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

[1] Frais de transaction, moyen et médian, en BTC et en USD, quotidien.

[2] Valeur cumulée, en USD, des récompenses d'émission monétaire et des frais de transaction perçus par les « mineurs ».

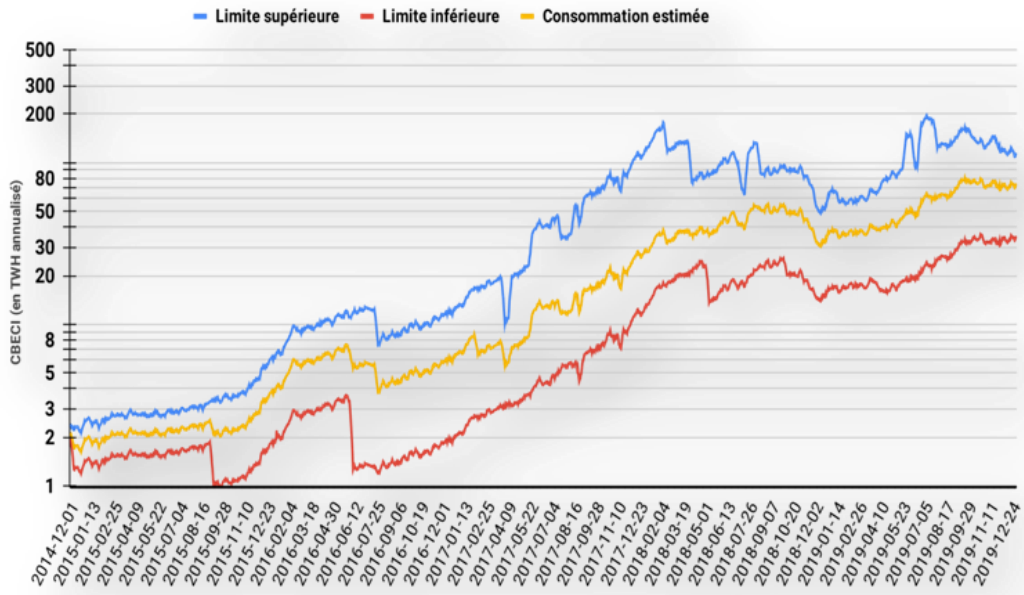
Annexe II.12 : Quantité Hash/s cumulée[1] et prix du BTC, en USD, quotidien

(de janvier 2009 à décembre 2019, échelle logarithmique



Annexe II.13 : Évolution de l'index de consommation électrique de Bitcoin, en TWH annualisé[2]

(de janvier 2009 à décembre 2019, échelle logarithmique)

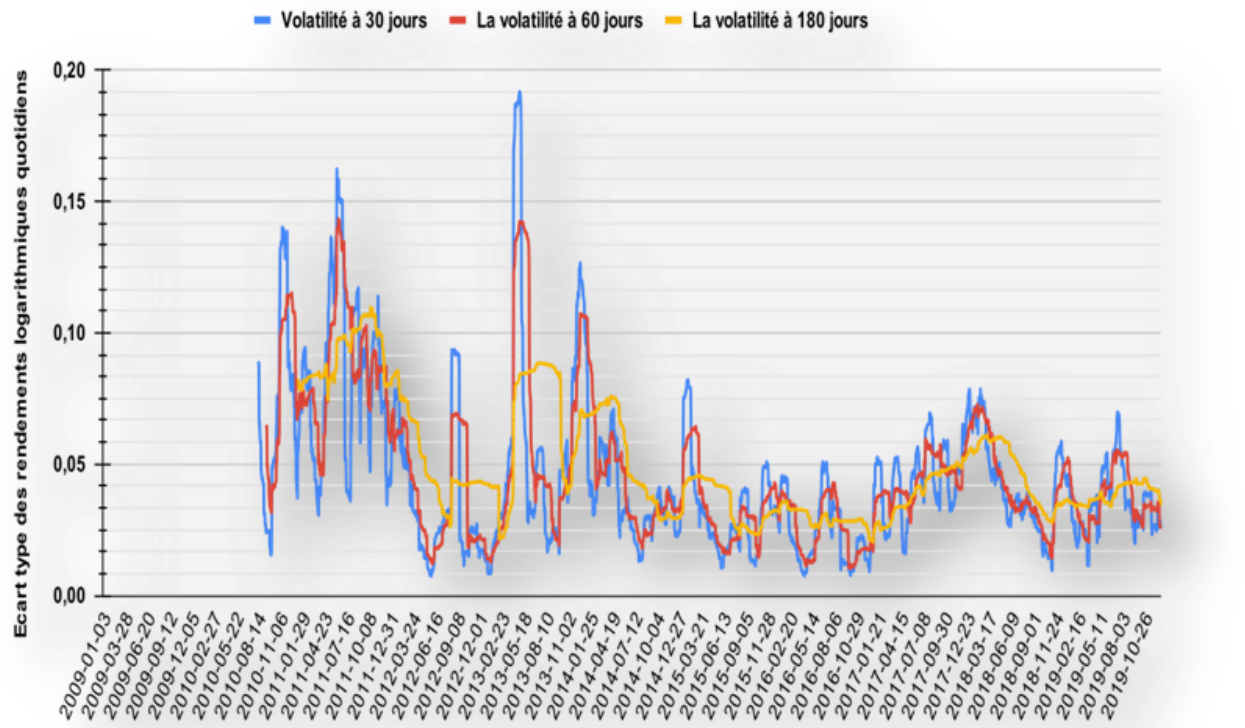


Source des données : https://www.coinmetrics.io; https://www.cbeci.org/ ; traitement de l'auteur.

[1] Taux de Hash moyen et quotidien déployé dans Bitcoin, exprimé en H/s.

[2] L'index de consommation électrique de Bitcoin (CBECI publié par Cambridge) : est un indicateur hybride combinant une liste d'équipements de minage type et des hypothèses concernant les seuils de rentabilité déterminant les équipements profitables en fonction du coût de l'électricité. Cela donne trois scénarios : (i) un optimiste (« limite inférieure » ou « *lower bound* »), représentant la limite inférieure, elle correspond au minimum de dépense électrique suivant l'hypothèse que tous les mineurs utilisent l'équipement le plus efficace ; (ii) un pessimiste (« limite supérieure » ou « *upper bound* ») correspondant à la dépense maximale de Bitcoin, suivant l'hypothèse que tous les mineurs utilisent le matériel le moins efficace énergétiquement, tant que l'exploitation de ce matériel reste rentable ; enfin, (iii) un scénario intermédiaire (« consommation estimée » ou « *best guess* »), reposant sur l'hypothèse que les mineurs utilisent un panier de matériel rentable plutôt qu'un modèle unique.

Annexe II.14 : Volatilité de l'UCN BTC, en USD sur 30, 60 et 180 jours[1]
(de janvier 2009 à mars 2021)



Source des données : https://www.coinmetrics.io; https://www.cbeci.org/ ; traitement de l'auteur.
[1] Volatilité de l'UCN BTC, en Dollars, calculée comme écart type des rendements logarithmiques naturels quotidiens sur 30, 60 et 180 jours.

Annexe III : Données synthétiques relatives à l'écosystème d'Ethereum

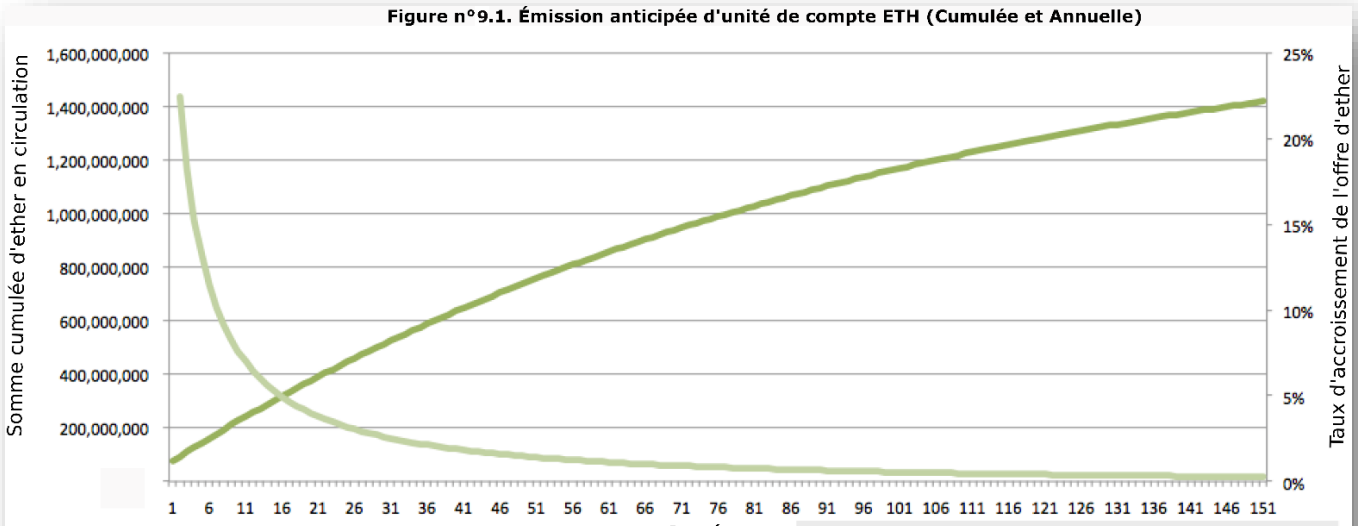
Tableau III.1: L'UCN Ether et sa décimalisation (matérielle et symbolique)

Ethereum et son UCN* Ether	
	
ETH **Ξ**	
Unité(s) fractionnaire(s) conventionnelle(s)	**Valeur en UCN* (ETH)**
L'« ***ether*** » | l' « *ETH* » | ou le « *Buterin* »	1 (Ou 10^{18} Wei)
Le « ***Milliether*** » | ou le « *Finney* »	0.001 (Ou 10^{15} Wei)
Le « ***Microether*** » | ou le « *Szabo* »	0.000001 (Ou 10^{12} Wei)
Le « **Gwei** » | le « *Shannon* » | ou le « *Nanoether* »	0.000000001 (Ou 10^{9} Wei)

Le « ***Mwei*** » | le « *Lovelace* » | ou le « *Picoether* »	0.000000000001 (Ou 10^6 Wei)
Le « ***Kwei*** » | le « *Babbage* » | ou « *Femoether* »	0.000000000000001 (Ou 10^3 Wei)
Le « ***Wei*** » | le « *Attoether* »	0.000000000000000001 (Ou 1 Wei)
Compilation de l'auteur ; https://gwei.io/ + https://coinguides.org/ethereum-unit-converter-gwei-ether/	

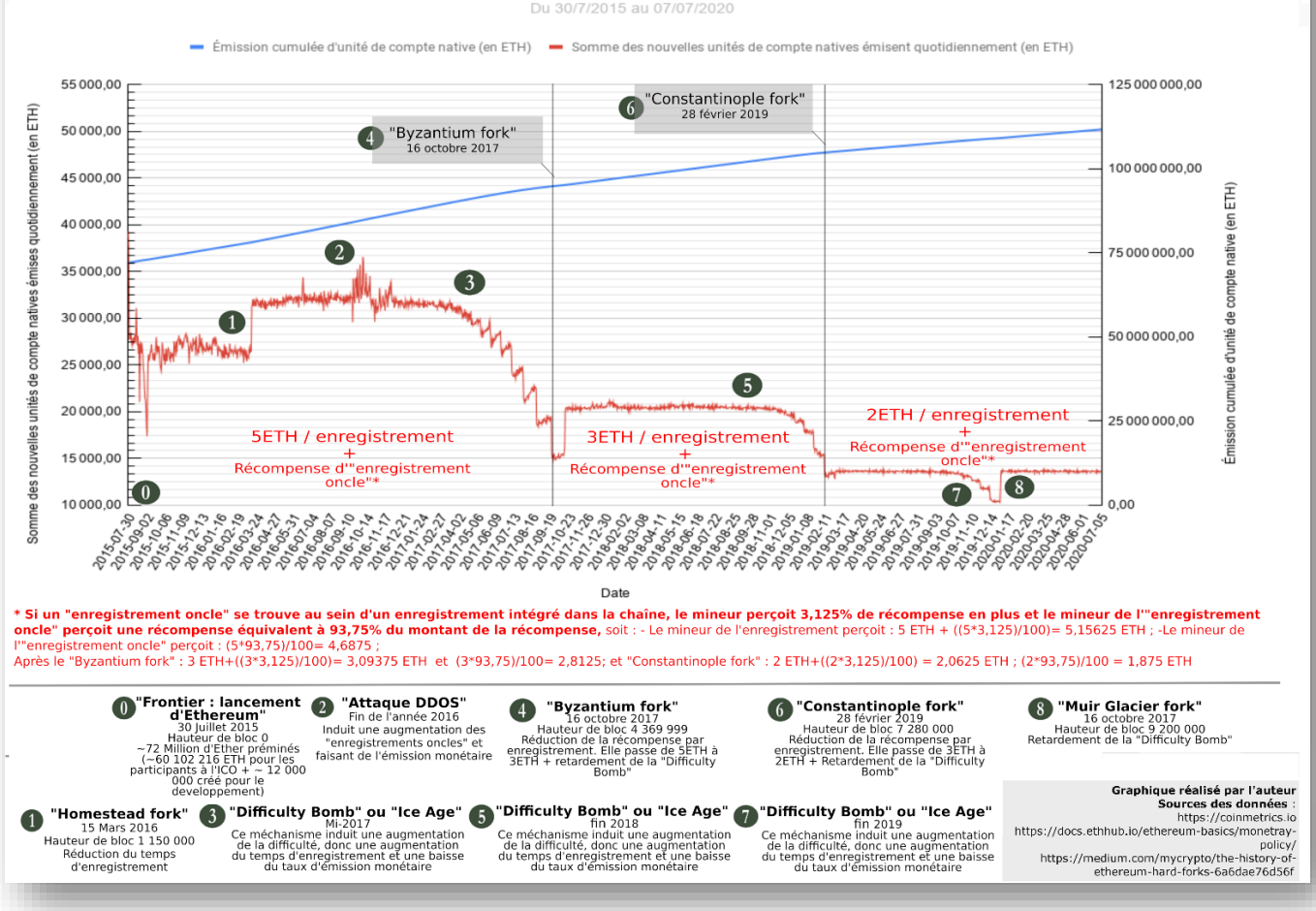
Annexe III.2 : l'offre monétaire programmatique d'Ethereum : entre émission anticipée et effective

Figure n°9.1. Émission anticipée d'unité de compte ETH (Cumulée et Annuelle)



Source : Graphique trouvé chez Lubin, 2014
voir https://blog.ethereum.org/2014/04/10/the-issuance-model-in-ethereum

Figure 9.2. Émission effective d'unité de compte ETH (Cumulée et quotidienne)



*** Si un "enregistrement oncle" se trouve au sein d'un enregistrement intégré dans la chaîne, le mineur perçoit 3,125% de récompense en plus et le mineur de l'"enregistrement oncle" perçoit une récompense équivalent à 93,75% du montant de la récompense,** soit : - Le mineur de l'enregistrement perçoit : 5 ETH + ((5*3,125)/100)= 5,15625 ETH ; -Le mineur de l'"enregistrement oncle" perçoit : (5*93,75)/100= 4,6875 ;
Après le "Byzantium fork" : 3 ETH+((3*3,125)/100)= 3,09375 ETH et (3*93,75)/100= 2,8125; et "Constantinople fork" : 2 ETH+((2*3,125)/100) = 2,0625 ETH ; (2*93,75)/100 = 1,875 ETH

0 **"Frontier : lancement d'Ethereum"**
30 Juillet 2015
Hauteur de bloc 0
~72 Million d'Ether préminés (~60 102 216 ETH pour les participants à l'ICO + ~ 12 000 000 créé pour le developpement)

2 **"Attaque DDOS"**
Fin de l'année 2016
Induit une augmentation des "enregistrements oncles" et faisant de l'émission monétaire

4 **"Byzantium fork"**
16 octobre 2017
Hauteur de bloc 4 369 999
Réduction de la récompense par enregistrement. Elle passe de 5ETH à 3ETH + retardement de la "Difficulty Bomb"

6 **"Constantinople fork"**
28 février 2019
Hauteur de bloc 7 280 000
Réduction de la récompense par enregistrement. Elle passe de 3ETH à 2ETH + Retardement de la "Difficulty Bomb"

8 **"Muir Glacier fork"**
16 octobre 2017
Hauteur de bloc 9 200 000
Retardement de la "Difficulty Bomb"

1 **"Homestead fork"**
15 Mars 2016
Hauteur de bloc 1 150 000
Réduction du temps d'enregistrement

3 **"Difficulty Bomb" ou "Ice Age"**
Mi-2017
Ce méchanisme induit une augmentation de la difficulté, donc une augmentation du temps d'enregistrement et une baisse du taux d'émission monétaire

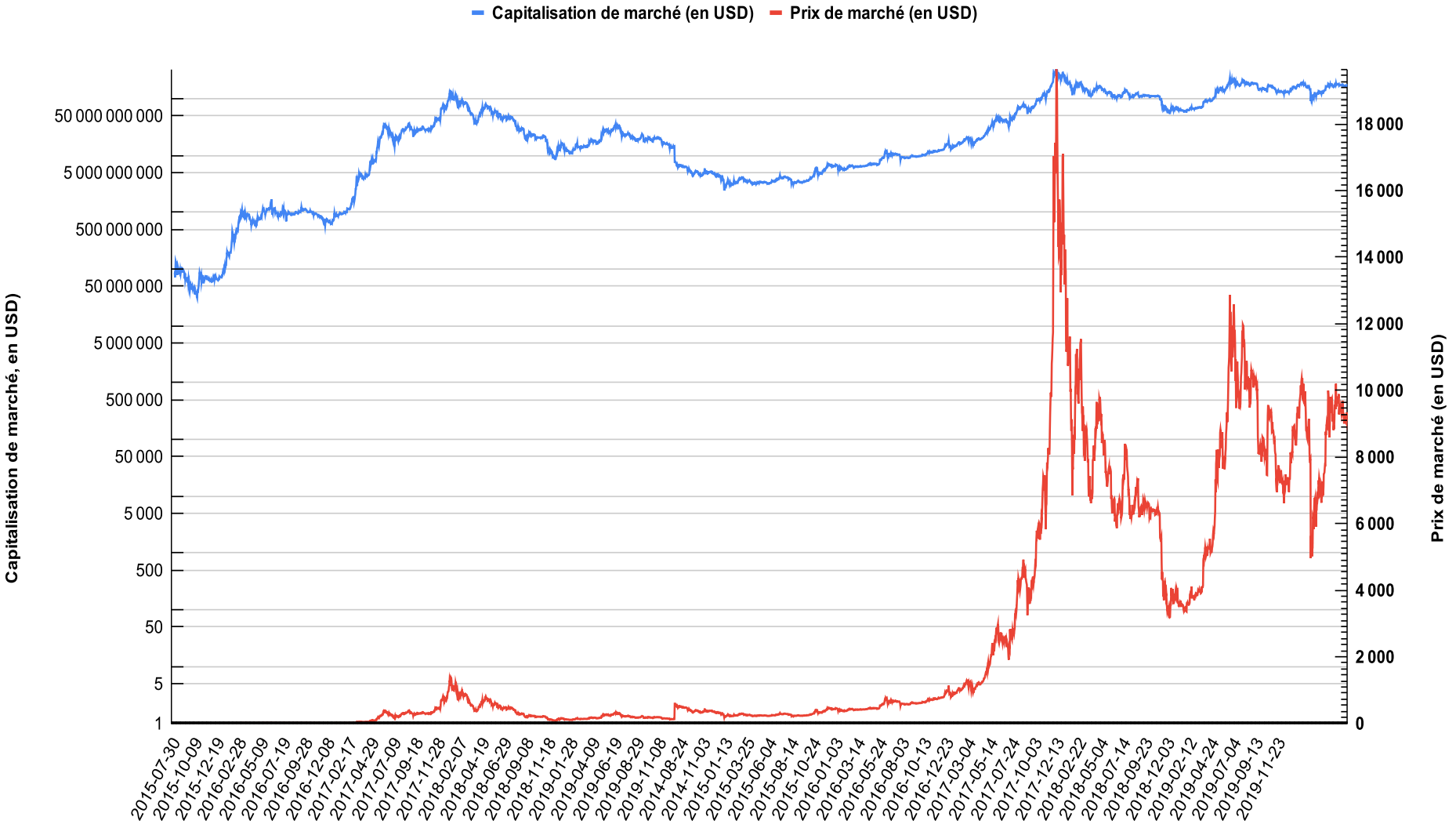
5 **"Difficulty Bomb" ou "Ice Age"**
fin 2018
Ce méchanisme induit une augmentation de la difficulté, donc une augmentation du temps d'enregistrement et une baisse du taux d'émission monétaire

7 **"Difficulty Bomb" ou "Ice Age"**
fin 2019
Ce méchanisme induit une augmentation de la difficulté, donc une augmentation du temps d'enregistrement et une baisse du taux d'émission monétaire

Graphique réalisé par l'auteur
Sources des données :
https://coinmetrics.io
https://docs.ethhub.io/ethereum-basics/monetray-policy/
https://medium.com/mycrypto/the-history-of-ethereum-hard-forks-6a6dae76d56f

Figure III.3 : Capitalisation de marché de l'ETH en prix de marché (1), en USD

(du 30 juillet 2015 au 01 janvier 2020)

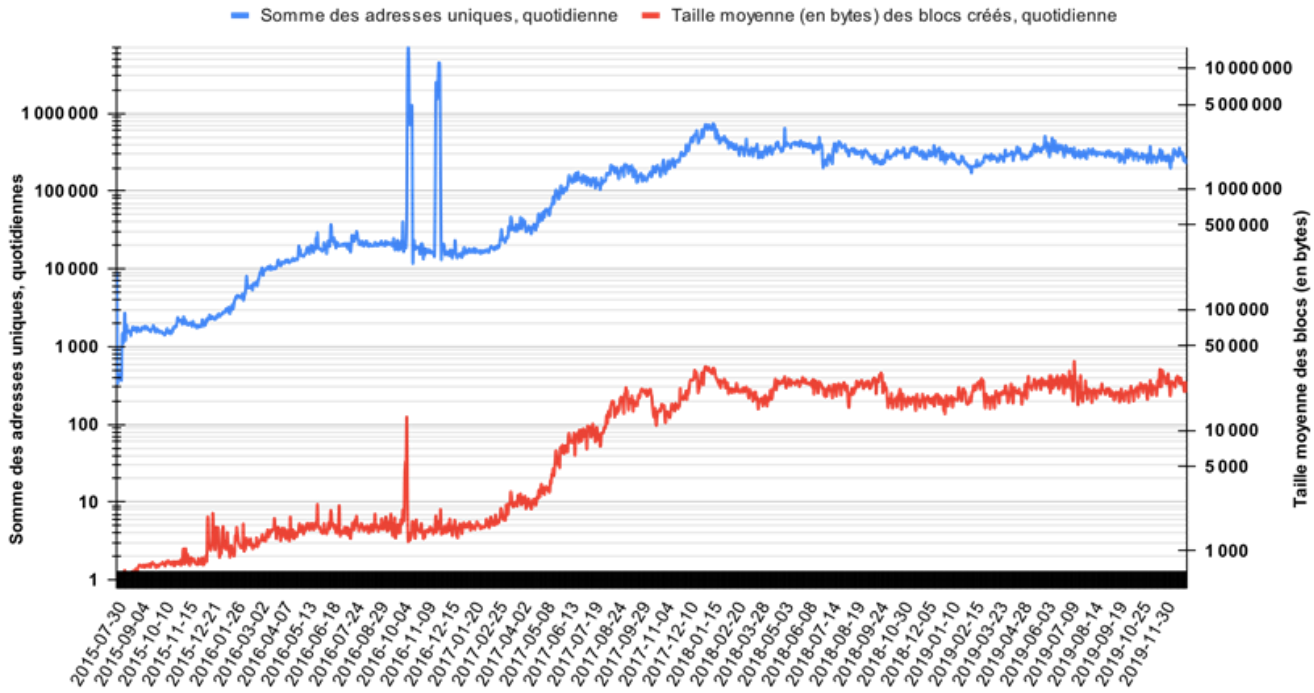


Source des données : https://www.coinmetrics.io; (Chapitre 1 pour la 1ère cotation) ; traitement de l'auteur.

(1) Capitalisation boursière « simple » : valeur agrégée en USD de l'offre actuelle, également appelée « valeur du réseau » ou « capitalisation du marché ».

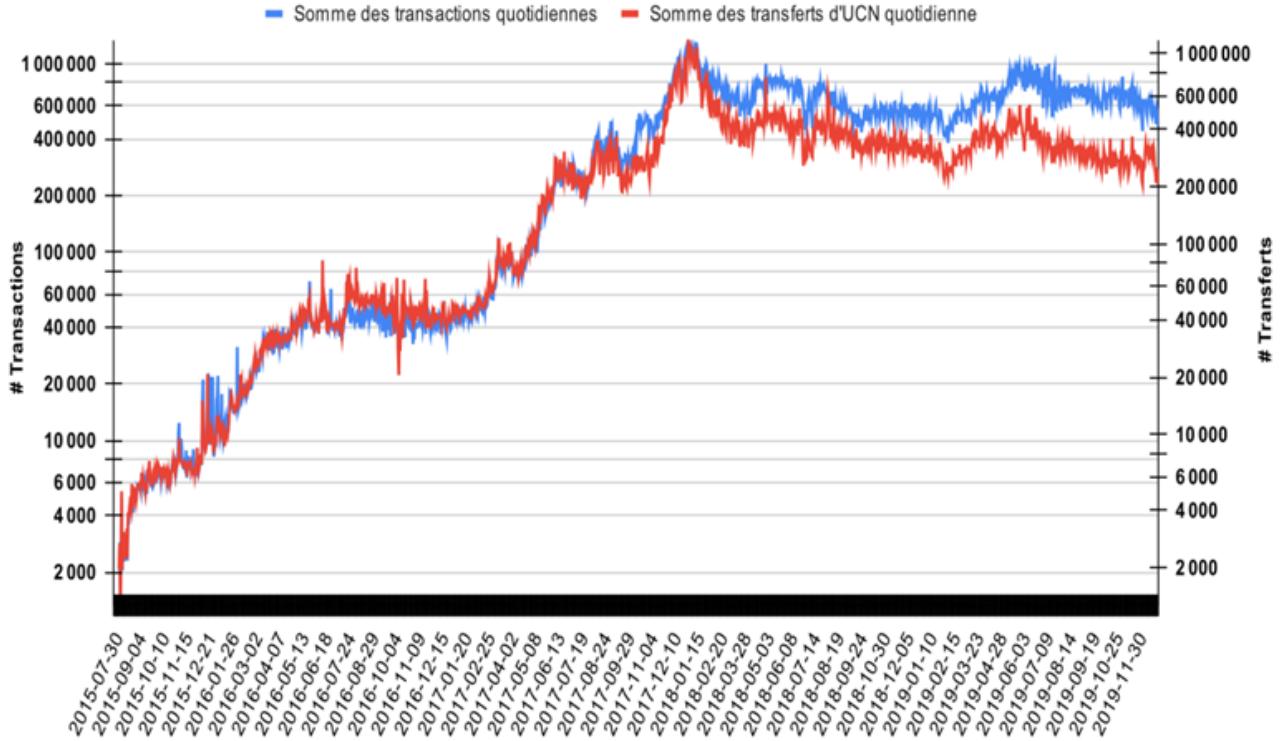
Annexe III.4 : Nombre d'adresses actives[1] et taille moyenne des enregistrements (en bytes), quotidien

(de juillet 2015 à décembre 2019, échelle logarithmique)



Annexe III.5 : Nombre de transactions[2] et transferts[3] quotidiens

(de juillet 2015 à décembre 2019, échelle logarithmique)



Source des données : https://www.coinmetrics.io; traitement de l'auteur.

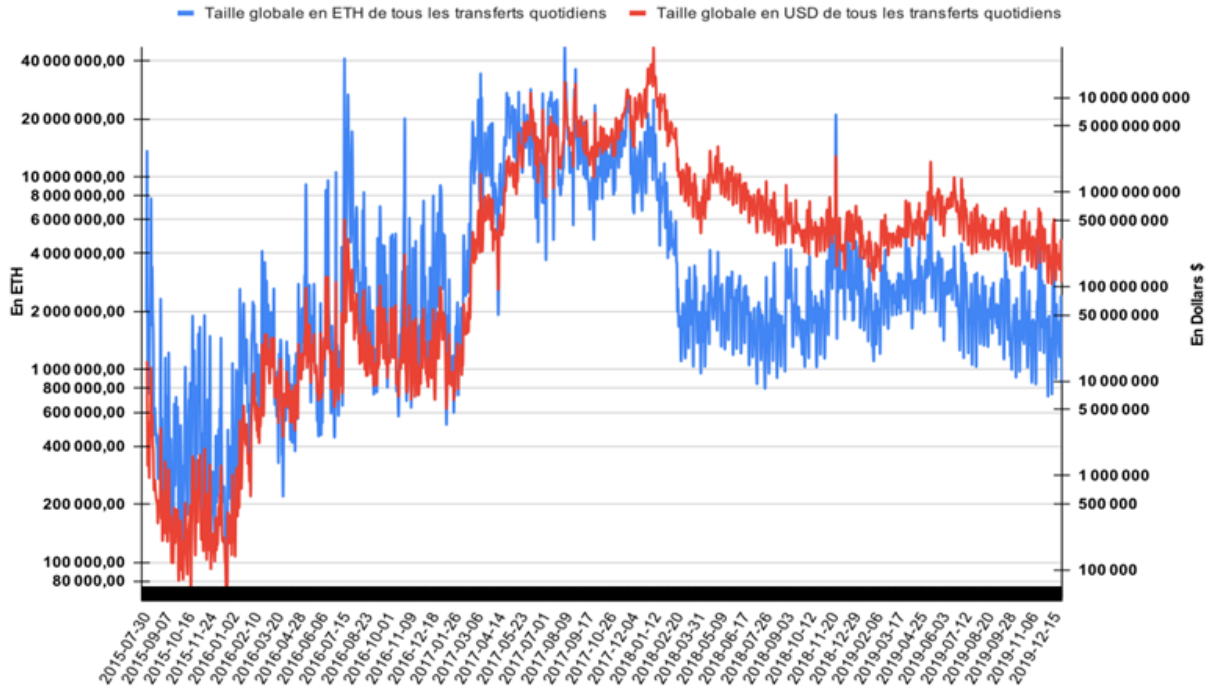
[1] Somme des adresses uniques actives quotidiennes (destinataires et envoyeurs, chaque adresse n'est comptée qu'une fois).

[2] Somme des transactions quotidiennes (exécutées ou non et avec transfert d'UCN ou non), hors transactions protocolaires.

[3] Somme des transferts quotidiens : mouvements d'UCN d'une adresse à une autre, résultants d'une transaction et qui ont une valeur positive.

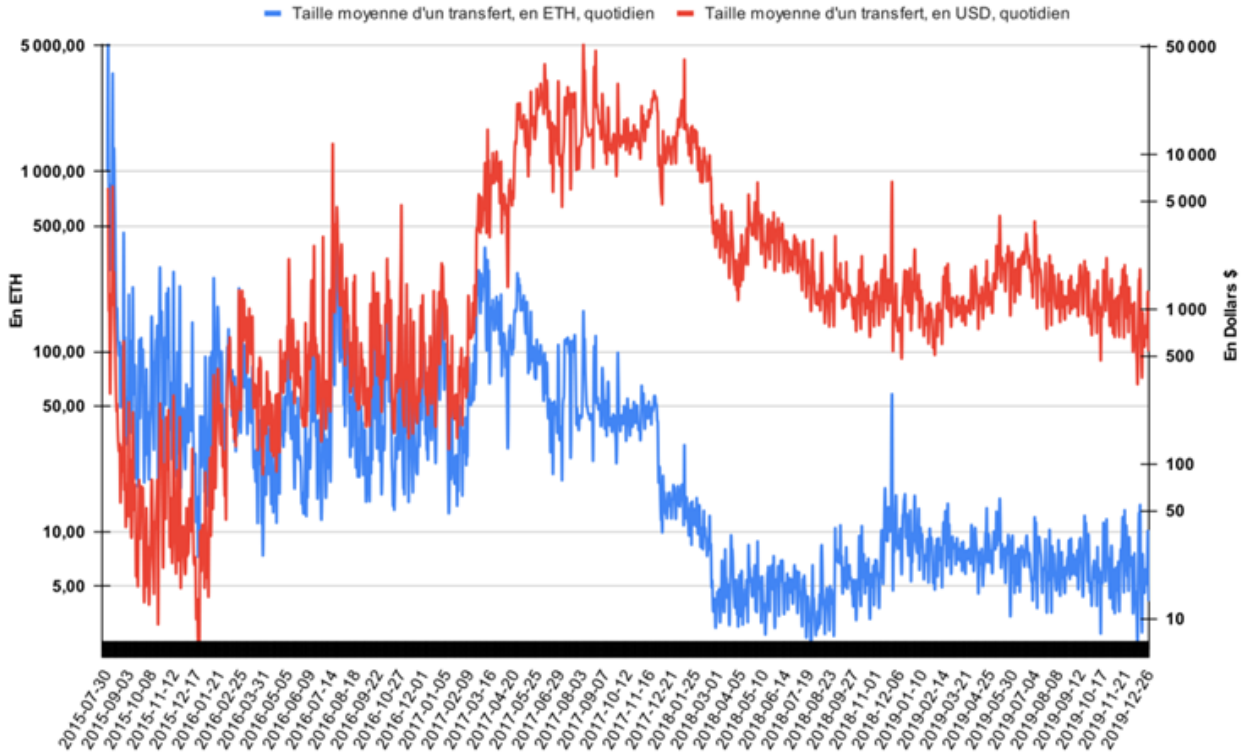
Annexe III.6 : Taille globale de tous les transferts quotidiens, ETH et USD[1]

(de juillet 2015 à décembre 2019, échelle logarithmique)



Annexe III.7 : Taille moyenne des transferts, en ETH et USD, quotidien[2]

(de juillet 2015 à mars 2019, échelle logarithmique)



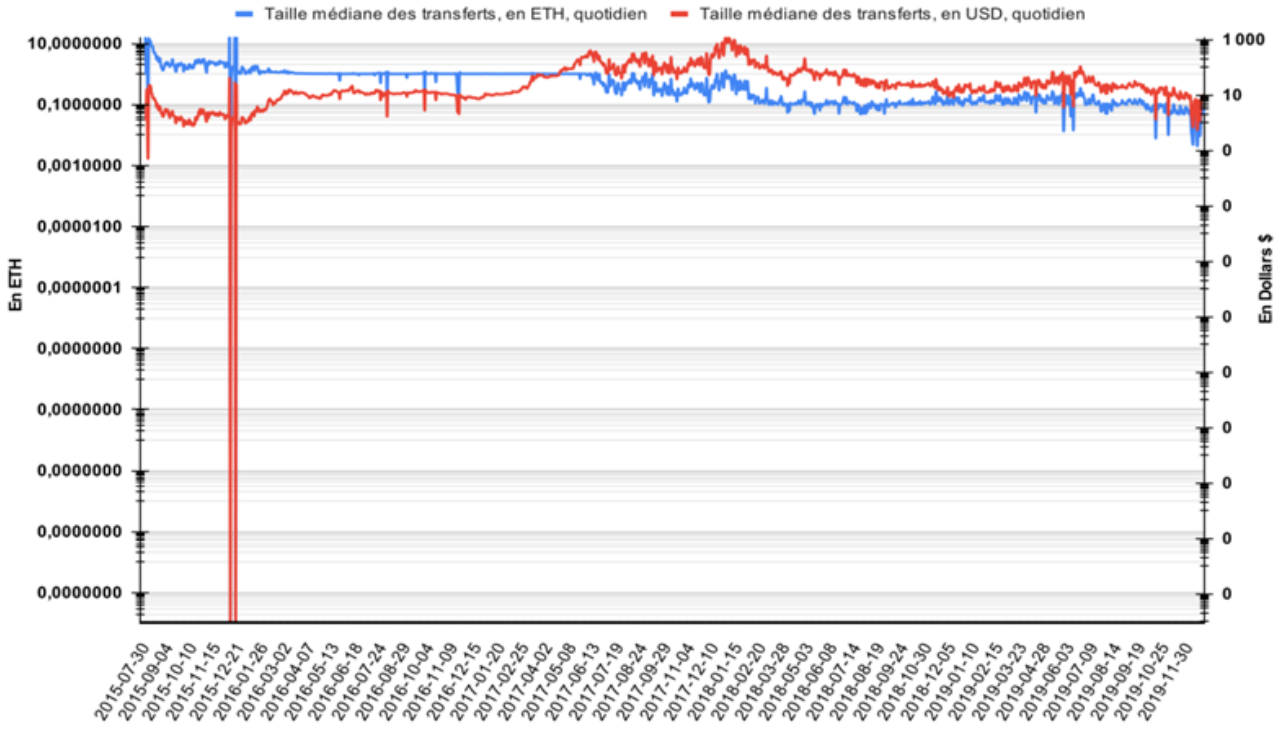
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

[1] Quantité totale d'UCN transférées (en ETH) et valeur agrégée des transferts (en USD), quotidienne.

[2] Quantité moyenne d'UCN transférée (en ETH) et valeur moyenne des transferts (en USD), quotidienne.

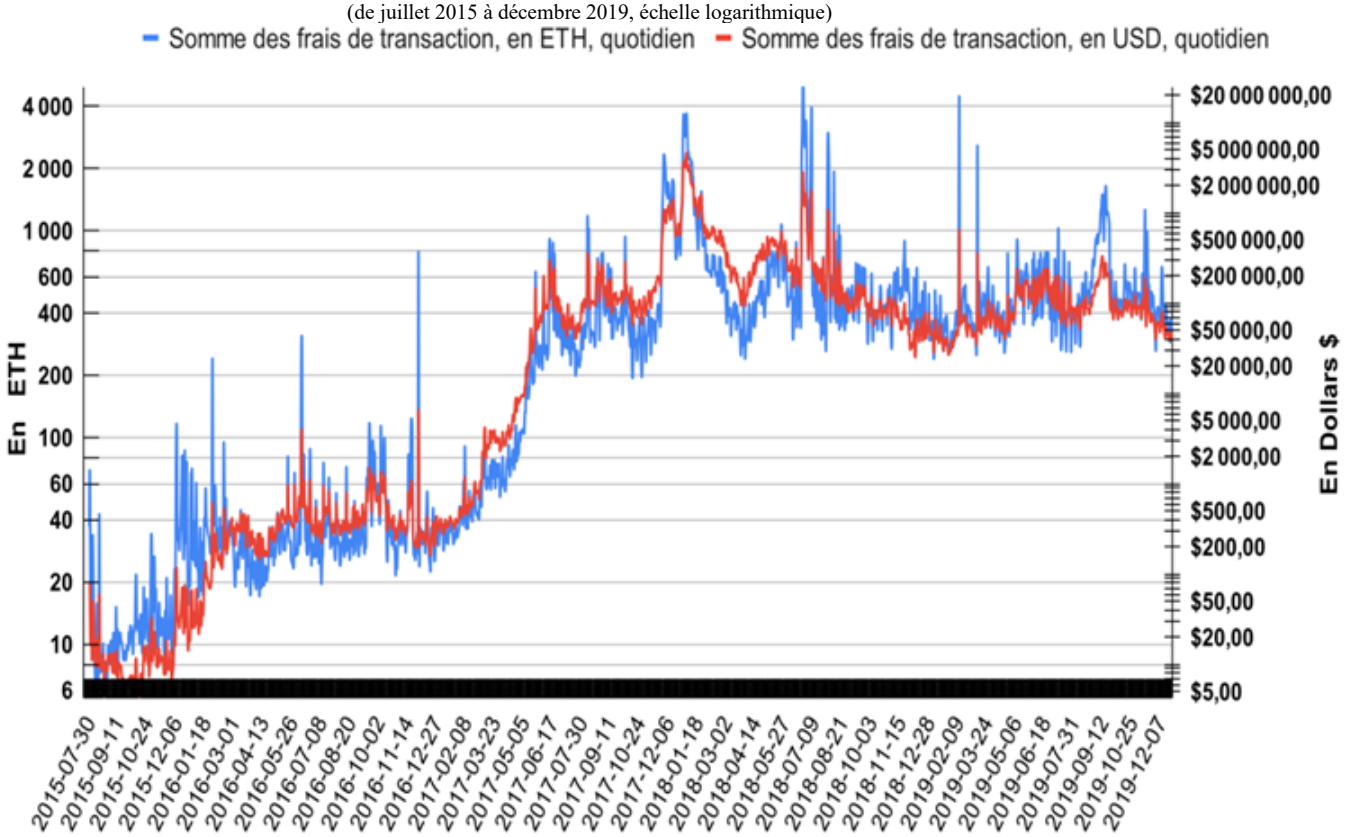
Annexe III.8 : Taille médiane des transferts, en ETH et USD, quotidien[1]

(de juillet 2015 à décembre 2019, échelle logarithmique)



Annexe III.9 : Somme des frais de transaction, en ETH et USD, quotidien[2]

(de juillet 2015 à décembre 2019, échelle logarithmique)



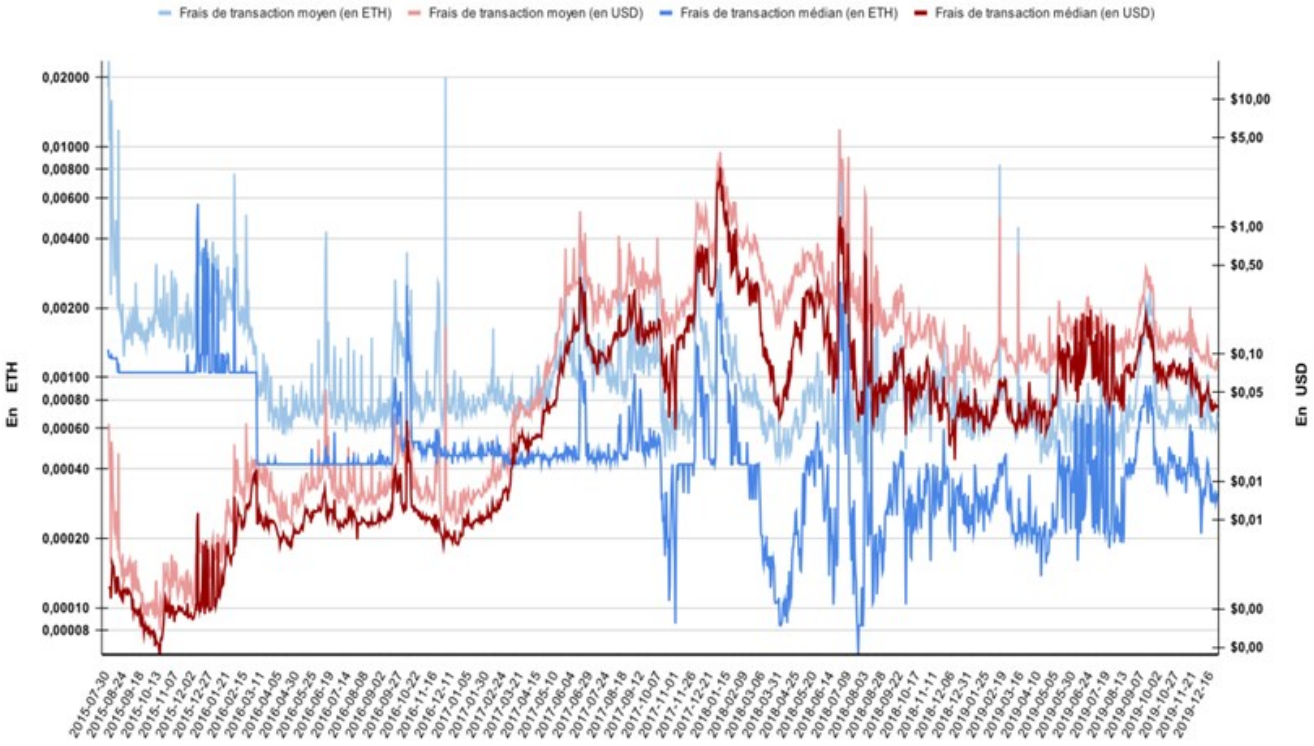
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

[1] Quantité médiane d'UCN transférée (en ETH) et valeur médiane des transferts (en USD), quotidienne.

[2] Somme des frais de transaction reçus par les mineurs, en ETH et USD, quotidien (hors récompenses d'émission monétaire).

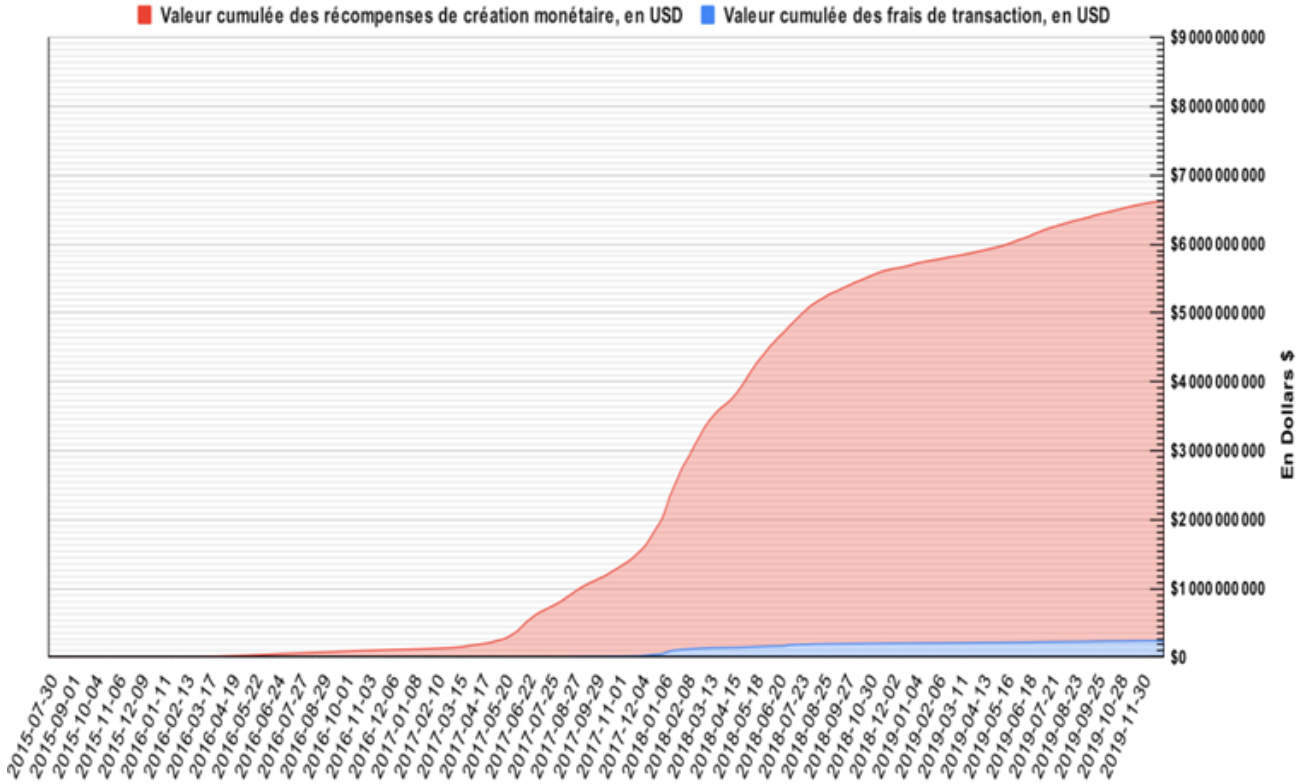
Annexe III.10 : Frais de transaction, moyen et médian, en ETH et USD, quotidien[1]

(de juillet 2015 à décembre 2019, échelle logarithmique)



Annexe III.11 : Revenu cumulé des « mineurs » en USD[2]

(de juillet 2015 à décembre 2019)



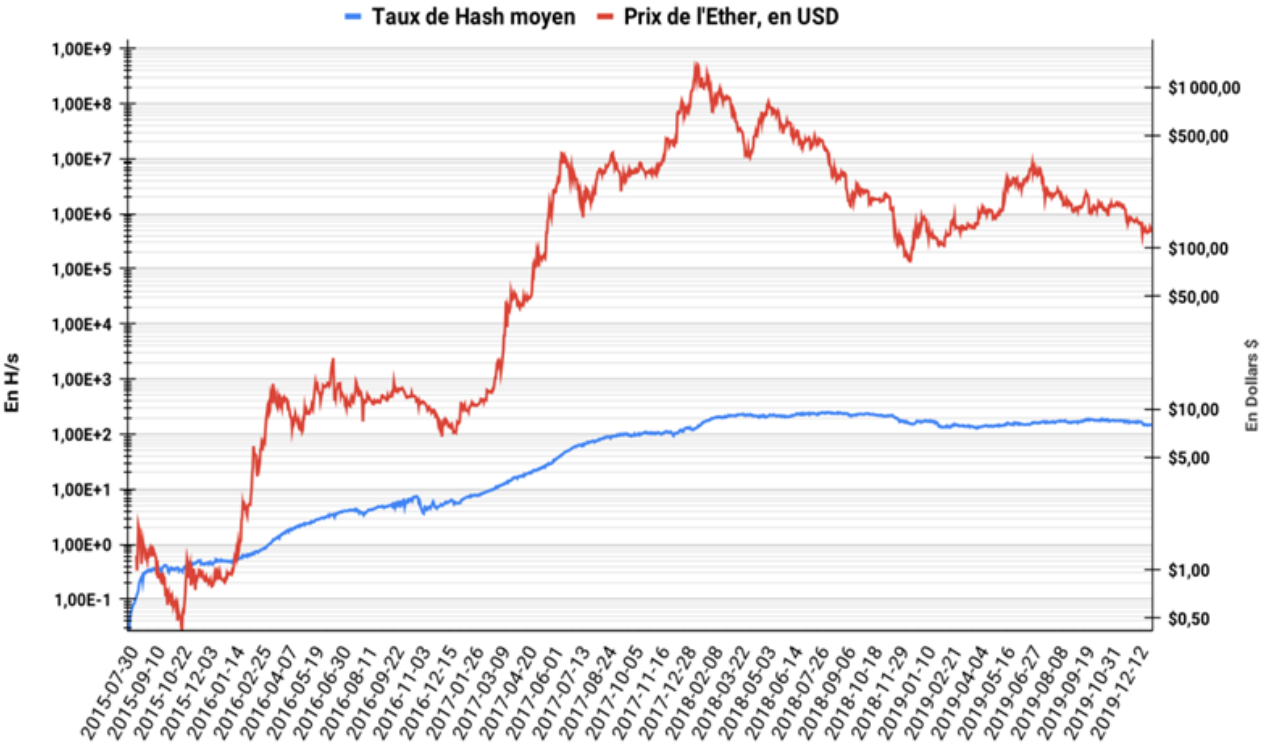
Source des données : https://www.coinmetrics.io; traitement de l'auteur.

[1] Frais de transaction, moyen et médian, en ETH et en USD, quotidien.

[2] Valeur cumulée, en USD, des récompenses d'émission monétaire et des frais de transaction perçus par les « mineurs ».

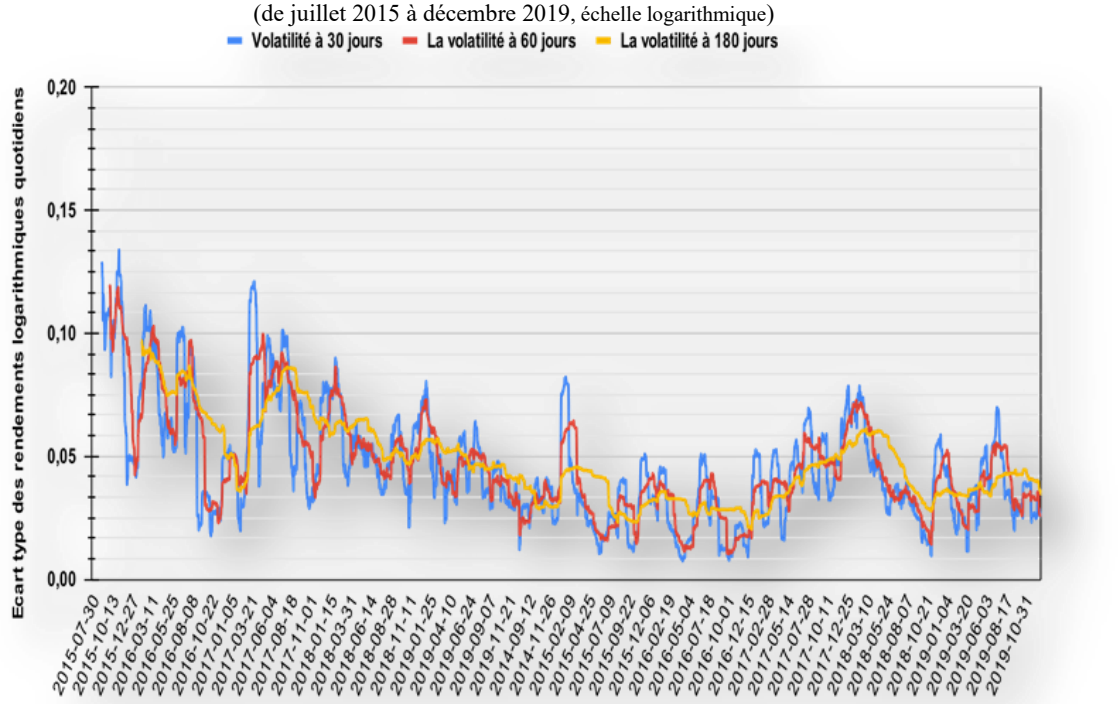
Annexe III.12 : quantité Hash/s cumulée[1] et prix de l'ETH en USD, quotidien

(de juillet 2015 à décembre 2019, échelle logarithmique)



Annexe III.13 : Volatilité de l'UCN ETH, en USD sur 30, 60 et 180 jours[2]

(de juillet 2015 à décembre 2019, échelle logarithmique)



Source des données : https://www.coinmetrics.io; https://www.cbeci.org/ ; traitement de l'auteur.

(1). Taux de Hash moyen et quotidien déployé dans Ethereum, exprimé en H/s.

(2). Volatilité de l'UCN ETH, en Dollars, calculée comme écart type des rendements logarithmiques naturels quotidiens sur 30, 60 et 180 jours.

Concernant l'absence de données sur la consommation électrique d'Ethereum : si un index similaire à celui de Bitcoin est aujourd'hui disponible (voir https://ccaf.io/cbnsi/ethereum, consultation au 05-02-2022), ces données ne couvrent pas la période qui est là notre. De fait, suivant qu'Ethereum a été conçu pour être à l'origine résistant aux ASICS (ils n'apparaîtront que tardivement), la méthodologie de cet indicateur a rendu difficile l'établissement d'une liste de machines de minage type (puisque n'importe quelle carte graphique d'ordinateur, même peu efficace, pouvait être utilisée initialement comme scénario type).

Annexe III.14 : Les cofondateurs d'Ethereum

Co-fondateur d'Ethereum	Biographie synthétique ***Sources*** *: Bradbury 2013; Munawa 2016; Summerwill 2018; Russo 2020; Hamacher 2020, synthèse de l'auteur*
Vitalik Buterin 	Il découvre Bitcoin en 2011, grâce à son père informaticien, Dimitry Buterin, alors qu'il n'a que 17 ans et est encore en études au Canada. Son intérêt pour Bitcoin le fera quitter ses études afin de se consacrer à temps plein à ses activités autour des CM. Féru de mathématique et d'informatique, il remporte en 2012 la médaille de Bronze des Olympiades Internationales d'informatique, reçoit en 2014 la bourse "Thiel fellowship" et, en 2018, reçoit à titre honorifique un doctorat en Commerce et Économie de l'Université de Bâle. Il va participer à Bitcoin en tant que programmeur - il a participé à différents projets (*darkwallet*, *KryptoKit*,, *Fork** de bitcoinjs-lib, *pybitcointools*, *multisig.info*, *Egora*, etc.) et auteur. En effet, avec Mihai Alisie, il co-fonde *Bitcoin Magazine* en 2012. Il travaille aussi sur la technologie des pièces colorées et sur Omni/Mastercoin. Depuis 2013, il travaille sur le développement Ethereum.
Mihai Alisie 	Diplômé en économie cybernétique à l'université de Lucian Blaga, Roumanie. A été coach et joueur de poker avant de découvrir Bitcoin en 2011. Suivant sa prise de contact avec V. Buterin, ils co-fondent *Bitcoin Magazine.* M. Alisie travaille sur une plateforme de vente en ligne dédiée à Bitcoin (Egora). Il va prendre part aux activités légales et administratives : installation en Suisse de la fondation Ethereum, ouverture de compte en banque, etc. Vice-président de la Fondation Ethereum jusqu'en 2015, il la quitte pour se consacrer à un nouveau projet, Akasha.

Antony Di Iorio 	Investisseur et entrepreneur, il est au contact de l'informatique depuis son plus jeune âge. Il obtient un diplôme en Management du Business à l'université de Ryerson. Disposant d'un capital économique familial important, il commence par être investisseur dans une entreprise de forage géothermique avant de découvrir Bitcoin. Il est l'organisateur, en novembre 2012, des premiers *"Bitcoin Meetup"* à Toronto, au sein desquels il rencontre V. Buterin. Il fonde l'organisation "Bitcoin Alliance Canada", comme le site de jeux en ligne "Satoshi Circle" qu'il revend en 2013. Il est en contact avec Hoskinson, qui a réalisé un programme éducatif autour de Bitcoin pour "Bitcoin Alliance Canada" : c'est lui qui lui transmettra la première version du projet. Du fait de son capital économique, il investit largement dans Ethereum, et plus largement dans cet écosystème. Il est CEO de "Decentral" (une bourse d'échange de CM canadienne) et de Jaxx (un service des premiers portefeuilles* multi-CM). Peu favorable au statut d'organisation à but non lucratif de la fondation, il se met en retrait du projet suite à cette décision.
Charles Hoskinson 	Mathématicien et entrepreneur, il a étudié la théorie analytique des nombres à l'université de Denver et de Colorado. Après un détour en politique comme bénévole de la campagne du candidat libertarien Ron Paul, il découvre Bitcoin en 2011. Intéressé par ses potentiels, il souhaite développer le premier DEX - "Decentralized Exchange", une bourse d'échange en P2P - pour les CM. En octobre 2013, cette idée aboutira au lancement, avec Dan Larimer, d'un protocole de registre* distribué *ad hoc*, "BitShare" dont Hoskinson est CEO et Larimer CTO. Ils développeront ensemble les concepts de "Distributed Autonomous Company" (DAC), ouvrant la voie à celui - central pour Ethereum aujourd'hui - des "Decentralized Autonomous Organisation" (DAO). En opposition avec Larimer, il quittera Bitshare au début 2014. On lui doit aussi l'établissement du "Cryptocurrency Research group" en septembre 2013 et la création du Comité éducation de la fondation Bitcoin, en août de la même année. Introduit à Ethereum et à Buterin par A. Di Iorio, il participe à son lancement. Son rôle principal sera la création de la fondation Ethereum, dont il sera nommé CEO en décembre 2013. Comme Di Iorio, il est opposé au fait que la fondation soit dotée d'un statut d'organisation non lucrative, ce qui conduit à des conflits avec les autres cofondateurs. Cela se traduira par son éviction en juin 2014. Il fondera avec Jeremy Wood, un ancien d'Ethereum, la société IOHK en 2015, dont il devient CEO. Opposé au Hard Fork* consécutif au Hack de "The Dao", il prendra part au projet Ethereum Classic (Ticker : ETC), né de la scission communautaire consécutive à la gestion de la crise. Il est aussi le fondateur du protocole de registre* distribué "concurrent" d'Ethereum Cardano (Ticker : ADA).

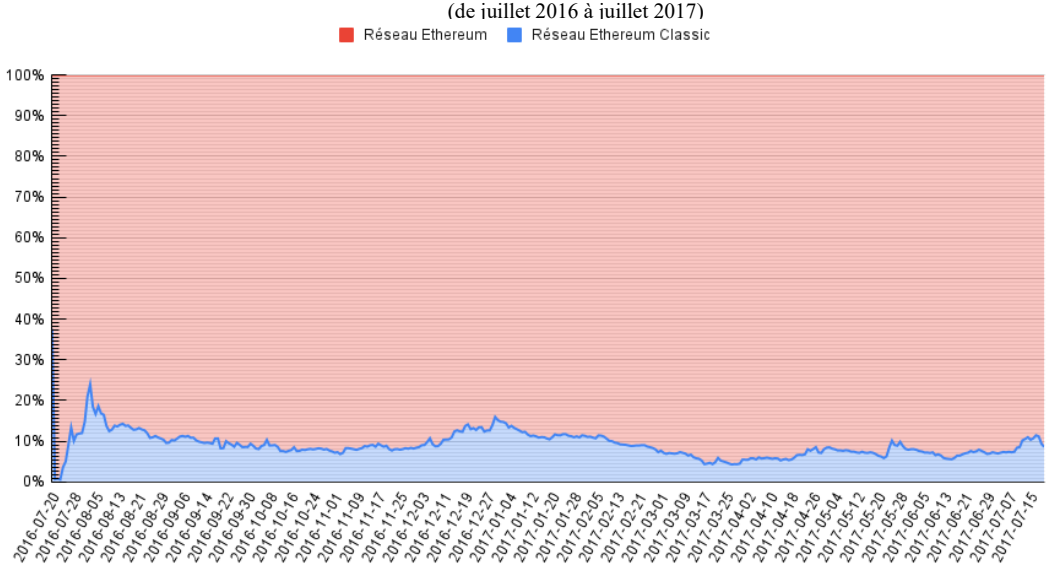
Gavin Wood 	Programmeur informatique et entrepreneur, il étudie la science informatique à l'université de York, où il obtient un doctorat en visualisation musicale. Passionné d'informatique et de jeux vidéo depuis son plus jeune âge, il est contributeur du mouvement des logiciels libres. Il découvre Bitcoin dans une vidéo avec Taaki et Alisie. C'est grâce à Taaki et une autre figure reconnue de la communauté, Johnny Bitcoin, qu'il est introduit au d'Ethereum. Il rencontrera Buterin, lui proposera d'implémenter le premier client Ethereum en langage C++, et sera le WP* premier à mettre en place un réseau* "testnet" Ethereum fonctionnel, ce qui lui permet de prendre une place, malgré quelques réticences, dans l'équipe des fondateurs. En avril 2014, il publie le *Yellow Paper*, qui vise à être une traduction du WP* de Buterin posant les spécifications techniques du protocole, de son réseau* et de l'*Ethereum Virtual Machine*. Il est aussi celui qui développa le langage de programmation* natif d'Ethereum : "Solidity". Il est CTO de la fondation Ethereum jusqu'en 2016 ; CEO de Parity technology, qui développe un client logiciel Ethereum codé en langage Rust ; fondateur de la "Web3 Fondation" et du projet de protocole de registre* distribué "concurrent" d'Ethereum Polkadot (Ticker : DOT).
Amir Chetrit 	Il a rencontré Buterin en 2013 lors d'une conférence Bitcoin et a travaillé pour la start-up Colored Coin, projet auquel a participé Buterin. Dès juin 2014, critiqué pour son manque de participation par les autres co-fondateurs et développeurs*, ayant proposé de se retirer, il est évincé comme Hoskinson.

Jeffrey Wilcke 	Programmeur informatique néerlandais qui avait travaillé pour le projet Mastercoin/Omni avant de s'intéresser à Ethereum. Motivé par ce projet, il réalise une implémentation logicielle en langage de programmation* Go, ce qui lui doit d'être ajouté à la liste des co-fondateurs - avec Wood - au début 2014. Ce premier client en Go - logiciel baptisé "Geth" aujourd'hui -, qui a été réalisé en même temps et sans concertation avec le développement du client en C++, impliqua qu'Ethereum eut, dès le départ, deux implémentations logicielles différentes et compatibles. Son retrait du projet Ethereum ferait suite aux nombreuses crises qu'Ethereum a pu traverser - la résolution de la crise de "The Dao Hack" par un Hard Fork* controversé, série d'attaques informatiques, etc. - et à des choix plus personnels. À son départ, il confie le développement du logiciel Geth à Peter Szilagyi, qui est encore aujourd'hui le développeur* principal du client Geth. Il travaille aujourd'hui avec son frère pour son propre studio de développement de jeux vidéo, qu'il a financé grâce à la vente d'une partie des Ether reçus pour sa participation au projet.
Joseph Lubin 	Détenteur d'un diplôme de génie électrique et informatique obtenu à Princeton, sa carrière va du génie logiciel à la production musicale, en passant par les affaires et la finance (Goldman Sachs's Private Wealth Management, BackSmith, co-fondateur d'un hedge fund). À Princeton, il a vécu en colocation avec Michael Novogratz, qui, à partir de 2015, sera connu - avec sa société Galaxie Digitale - pour ses activités d'investissement dans le secteur des CM. Il s'intéresse aux CM et prend contact avec son compatriote A. Di Iorio par le biais de la "Bitcoin Alliance of Canada". C'est lors de *"Bitcoin meetup"* à Toronto qu'il rencontre Buterin. Disposant d'un capital économique, il va avec Di Iorio assurer le financement du jeune projet. Si le choix a été fait de doter la fondation Ethereum - en charge du développement du projet - du statut d'organisation à but non lucratif, et suivant le fait que Lubin envisageait dès le départ que la couche applicative sur Ethereum devait être liée à une logique lucrative, il fonde l'entreprise "Consensys" dès 2014, qui joue un rôle de premier plan dans le financement et l'incubation de start-ups du secteur Blockchain. Lubin, va ainsi jouer un rôle clé dans le démarchage de partenaires d'Ethereum, tels que JPMorgan, CME Group, BNY Mellon, Credit Suisse, Banco Santander, BBVA, ING, UBS, BP, Intel et Microsoft. Le 28 février 2017, "Consensys" fait partie - comme Accenture, Banco Santander, BlockApps, BNY Mellon, CME Group, ConsenSys, IC3, Intel, J.P. Morgan, Microsoft, BBVA, BP, Crédit Suisse, Fubon Financial, ING, Monax, Tendermint, Thomson Reuters, UBS, etc. - des membres fondateurs de l' "Entreprise Ethereum Alliance", une organisation visant à promouvoir le développement d'Ethereum pour les entreprises.

Annexe III.15 Ethereum Versus Ethereum Classic

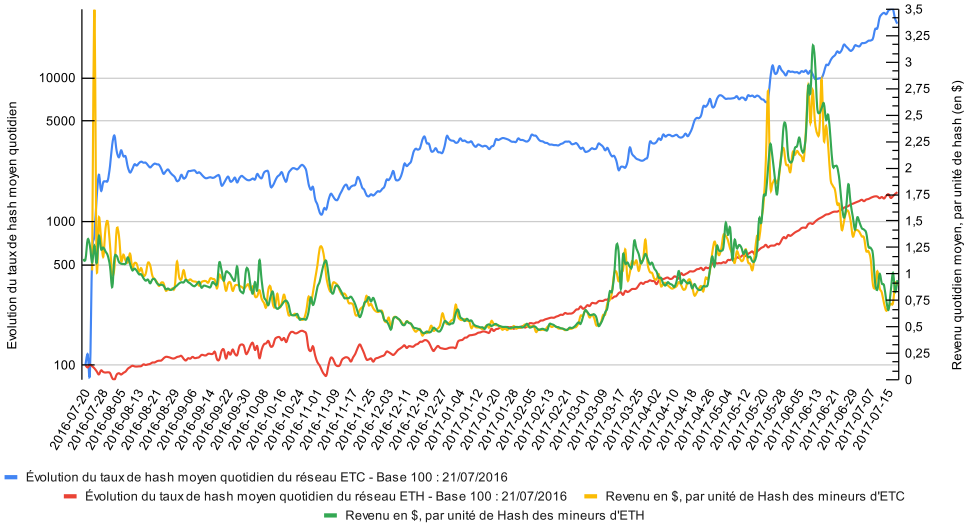
Annexe III.15.1 : Répartition du taux de Hash moyen entre ETH et ETC, quotidien (1)

(de juillet 2016 à juillet 2017)



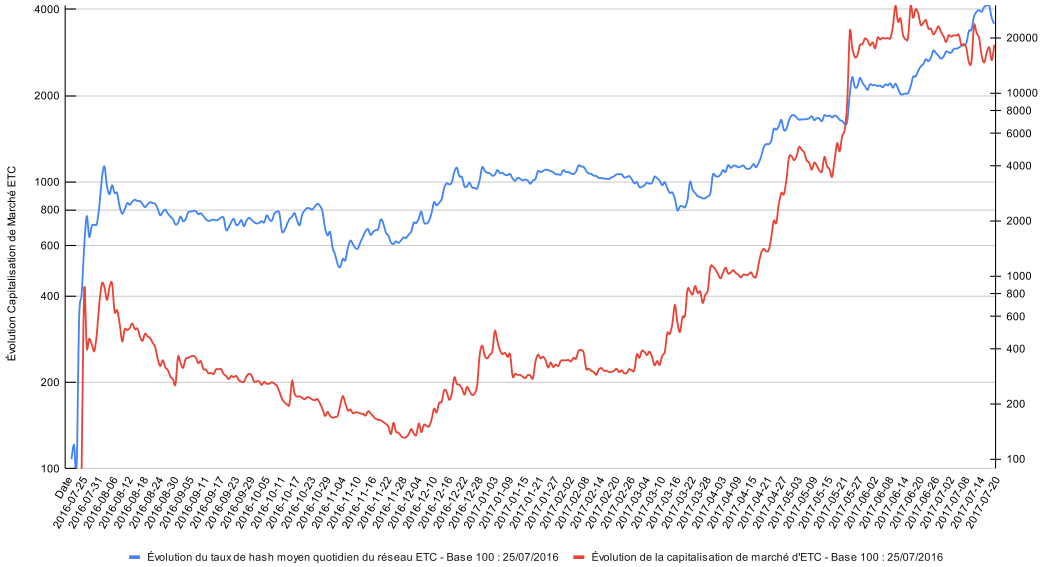
Annexe III.15.2 : Miner de l'ETH ou de l'ETC : un dilemme philosophique et économique (2)

(de juillet 2016 à juillet 2017)



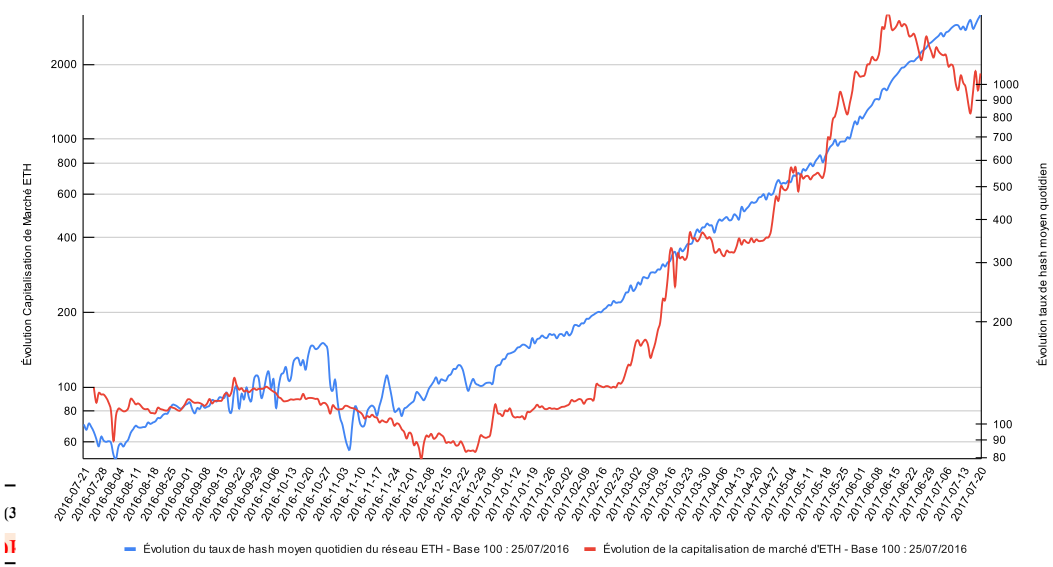
Annexe III.15.3 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum Classic(3)

(de juillet 2016 à juillet 2017, échelle logarithmique)



Annexe III.15.4 : Évolution du taux de Hash moyen quotidien et capitalisation de marché d'Ethereum (4)

(de juillet 2016 à juillet 2017, échelle logarithmique)



Annexe IV: Données synthétiques relatives à nos stratégies et dispositifs d'accès au terrain

Annexe IV.2 : Détails des immersions participantes

Il serait impossible et fastidieux de réaliser une liste exhaustive de nos différentes expériences en ligne – *on chain** et *off chain** - ; aussi, ce tableau vise à ramasser certaines des expériences clefs, tout en soulignant les compétences impliquées acquises et/ou mobilisées.

Période	Type d'activité	CM impliquée et type d'interaction en ligne	Connaissance(s) impliquée(s)
Fin 2015	Création d'un portefeuille Bitcoin	Bitcoin Hors-protocole*	Initiation aux principes de base du fonctionnement du Bitcoin, tels que la génération et la gestion des clés privées et publiques, la création et la diffusion des transactions*, la notion d'UTXO*, etc., *via* la découverte du portefeuille Electrum : téléchargement *via* Internet, installation du logiciel client ; création d'une adresse Bitcoin et sécurisation de la « seed » (sur papier) ; réception et envoi de BTC ; découverte des UTXO* et de leur implication en termes de frais de transaction* pour les transactions* futures (voir infra « Faucet »).

Fin 2015-2016	Obtention de nos premières UCN* *via* “Faucet”	Bitcoin et autres Hors-protocole* et au sein du protocole*	Obtention des premières UCN* v*ia* site de micro-dons (les « faucets ») et compréhension pratique de la gestion des UTXO* ; exploration de l’écosystème crypto-monétaire avec ses différents types de CM (générations, caractéristiques, usages, etc.) ; compréhension des enjeux liés à l’interopérabilité, à la scalabilité, à la sécurité, etc. ; sensibilisation aux aspects communautaires, économiques, culturels, éthiques, etc. des différentes CM. Premières transactions* vers notre portefeuille Bitcoin : effet « whaou », suivant la découverte du suivi en temps réel, du traitement de la transaction* en ligne *via* un explorateur de Blockchain, visualisation des confirmations participant de la finalisation conventionnelle du transfert ; découverte de la traçabilité des UTXO* utilisées depuis leur origine (cf. transaction* *coinbase* qui les ont émises) ; appréhension pratique du mécanisme des frais de transaction* et de la structure des UTXO* qui constituent les fonds de son portefeuille : certains sites permettent d’accumuler les récompenses *off chain**, d’autres transfèrent directement les fonds *on chain*,* à chaque action réalisée. Les premiers évitent, au prix d’une centralisation, les coûts induits par ces micro-paiements : directement, car chaque micro-paiement doit s’acquitter de frais forcément élevés rapportés à leur valeur propre et indirectement, car recevoir une multitude d’UTXO* de faible valeur se traduit à l’avenir par des transactions* lourdes, donc chères, car constituées d’un grand nombre d’UTXO* de petit montant (d’où l’appellation de « dust » pour les UTXO* plus couteux à récupérer que ce qu’ils ne valent). Création d’autre portefeuille pour les autres CM et premières transactions*, appréhension des points communs et des différences d’architecture (temps d’enregistrement*, frais de transaction*).

Janvier 2016	Teste minage de BTC	Bitcoin Hors-Protocole* : installation d'un client de minage (échec)	Confrontation aux contraintes matérielles et logicielles du minage de Bitcoin, telles que la puissance de calcul, la consommation électrique, le système d'exploitation, le choix du logiciel, la configuration du réseau*, etc. : échec lié aux difficultés techniques (problème de compatibilité avec mon ordinateur sous Linux).
Janvier 2016	Premier achat de BTC sur la plateforme en ligne VirWox	Hors-Protocole* : achat sur la plateforme et attente que le BTC/USD augmente afin que les frais de sortie exprimés en BTC ne soient pas trop importants Au sein du protocole* : transaction* de sortie	Découverte d'une première plateforme d'échange en ligne BTC contre fiat – Virwox, originellement conçue pour la monnaie numérique du jeu « Second life » – et de ces modes de paiement, de ces frais, etc. ; confrontation aux notions de taux de change, de liquidité, etc. ; Expérience du transfert de Bitcoin entre les plateformes et les portefeuilles* personnels, de la gestion des délais, des confirmations, des frais. Cf. les BTC achetés ont été retirés après un temps long (trois ans), pour éviter des frais, nominalement exprimés en BTC, trop importants : exprimés en $, ils étaient très élevés en BTC au moment de leur achat, et ont baissé suivant l'appréciation du cours.
10-02-2016	Création d'un compte sur Kraken, puis sur d'autres bourses d'échange (Coinbase, Poloniex, Bitfinex, Cryptopia, Liqui, Tux, etc.)	Hors-Protocole* : achat sur différentes plateformes Au sein du protocole* : transaction* d'entrée/sortie entre adresse et compte	Découverte de la diversité des plateformes d'échange de CM ; confrontation aux différentes offres de paires de trading (CM et/ou de fiat monnaies), des conditions d'enregistrement plus ou moins exigeantes (cf. divulgation d'identité), des modes de paiement, des frais afférents, des risques (« Cryptopia » a fermé suite à un Hack et nos fonds, de faible valeur, ont été perdus) et des avantages relatifs ; confrontation à la pratique du trading et ses concepts (taux de change, liquidité, volatilité, *spread*, *slippage*, *bid* et *ask*, *market order*, le *limit order*, etc.) ; confrontation aux contraintes liées à l'achat/vente de CM et au transfert de celles-ci entre adresses personnelle et compte de plateforme (coûts et délais de confirmation différents suivant les CM, etc.) ; diversification des CM détenues et exploration de la galaxie des Altcoins* présentée en Chapitre I.

01-10-2016	Achat de contrat de minage chez Genesis Mining (Dash, Bitcoin, Ethereum, Zcash)	Hors-Protocole* : achat sur différentes plateformes Au sein du protocole* : transaction* de sortie vers nos adresses et/ou compte	Suite à l'échec de notre tentative de minage personnel, découverte du minage en nuage (cloud mining), des différentes offres (contrats de location différents, pour différentes CM), des coûts et frais afférents, des rendements (très largement décroissants) et des contraintes en termes de rentabilité : évaluation des CM minées en fonction de leurs caractéristiques, de leurs algorithmes, de leurs difficultés, des prix, etc. ; suivi des performances et des revenus du minage en nuage et de leur grande dépendance à l'évolution du marché et à la concurrence entre mineurs (arrivée de nouvelles machines rendant les anciens contrats non rentables).
De mai 2016 à mai 2017	Activité de minage individuel sur mon ordinateur portable *via* Minergate	Bitcoin, Ethereum, Zcach, etc. Hors-Protocole* : Installation d'un client de minage « en un click » Au sein du protocole* : transaction* de sortie vers adresses ou compte	Retour sur minage individuel *via* expérimentation d'un logiciel dédié aux utilisateurs non techniciens : confrontation aux contraintes matérielles (chauffe et bruit), aux différents paramètres possibles entourant la répartition des récompenses entre hash*eurs d'une même pool de minage; là encore, sélection des CM à miner, suivant leurs caractéristiques et les performances en termes de revenu.
	Beta-testeur pour Spell of Genesis	Bitcoin, Counterparty Hors chaîne* : installation d'un client logiciel et échanges avec les développeurs* Au sein du protocole* : réception de BTC et de *tokens* sur un portefeuille Counterparty	Participation à la phase de test d'un jeu vidéo basé sur la blockchain Bitcoin et le meta protocole Counterparty (cf. Chap I) ; découverte et échange avec des acteurs d'un écosystème souhaitant développer des activités économiques autour des propriétés de Bitcoin (micro-paiement, in games tokens et CM) ; gain en nature sous forme de jetons numériques du jeu (CM native et tokens) ; découverte du gameplay, des graphismes, des scénarios, des personnages, des cartes, des quêtes, des récompenses, qui tournent autour de la culture crypto et de son histoire ; confrontation aux aspects techniques, ludiques, artistiques, économiques, sociaux, etc. ; confrontation aux difficultés posées par l'augmentation des frais de transaction* Bitcoin.

	Beta-testeur pour Storj	Bitcoin, Counterparty Hors chaîne* : installation d'un client logiciel, partage de notre disque dur en P2P et échanges avec la communauté Au sein du protocole* : réception de la CM native en guise de revenu de location et récompense de participation sur un portefeuille Counterparty	Participation à la phase de test d'un service de stockage cloud décentralisé – SorJ – utilisant le métaprotocole Counterparty basé sur Bitcoin ; installation d'un client logiciel, partage du disque dur en P2P afin de participer au réseau* de stockage ; échanges avec la communauté de testeurs ; réception de la CM native (STORJ) en guise de revenu de location et de récompense de participation, sur un portefeuille Counterparty ; connaissance des aspects techniques, économiques, sociaux, etc. du stockage cloud décentralisé ; confrontation aux difficultés posées par l'augmentation des frais de transaction* Bitcoin, le projet migre vers Ethereum (cf. Chap 1).
De 2016 à 2017	Participation au projet "Rare Pepe Cards" sur la plateforme CounterParty	Bitcoin, Counterparty Hors chaîne* : création de nos premiers tokens/NFT, achat / vente et don /contre-don au sein de la communauté Au sein du protocole* : réception/ envoi de CM et tokens, achat et vente *via* DEX Counterparty	Participation à un projet communautaire artistique et ludique, basé, là encore, sur le métaprotocole Counterparty : on retrouve dans le chat Telegram les acteurs importants des communautés Spell of Genesis, Storj et, plus généralement, des différents projets lancés sur Counterparty ; réception de la CM native Pepecash en don, nous permettant de créer et payer les frais de soumission de notre première carte numérique de collection (tokens/NFT), représentant des variantes du même Pepe ; création de nos premiers tokens/NFT, en utilisant le protocole Counterparty et en respectant les critères de rareté et de qualité ; achat, vente, don et contre-don des cartes au sein de la communauté : réception et envoi de CM (Bitcoin, XCP, Pepecash) et de tokens/NFT (nous en avons créé trois au total), en utilisant un portefeuille compatible ; premier achat et vente de tokens/NFT *via* le DEX (Decentralized Exchange) de Counterparty, qui permet de faire des transactions* directement *via* le protocole ; connaissance des aspects techniques, artistiques, culturels, économiques, sociaux, etc. du projet Rare Pepe Cards et des controverses l'entourant à l'époque (récupération de ce symbole par l'extrême-droite et volonté de la communauté Rare Pepe de contester cette récupération). Appréhension très réelle de l'opprobre que certains Bitcoiners* rencontrés aux *Meet Up* jettent à ces usages.

De 2016 à 2019	Investissement dans des ICO	Ethereum, mais aussi Bitcoin via Counterparty Hors chaîne* : découverte de la galaxie d'Altcoin* qui continue d'émerger Au sein du protocole* : réception/ envoi de CM	Participation à des levées de fonds en CM - les ICO ou *Initial Coin Offering* - qui permettent de financer des projets basés sur la blockchain ; confrontation à la croissance extensive et intensive de l'écosystème avec les différent(e)s caractéristiques, usages, valeurs, des CM et crypto-actifs* lancés, etc. ; réception et envoi de CM (ETH surtout, BTC un peu), en utilisant des portefeuilles* compatibles avec les protocoles des projets financés par les ICO; confrontation aux opportunités et risques liés aux ICO, tels que le potentiel de croissance et retour sur investissement important, mais aussi les pertes tout aussi importantes, voire totales, les questions de régulation, de sécurité, d'escroquerie : participation à des ICO plus ou moins réussies, telles que Mycelium, The DAO, Vslice, Bancor, BTU Protocol, etc. ; analyse critique des projets, de leurs objectifs et réalisations effectives, de leurs échecs et des leçons tirées ou non par le projet lui-même ou ceux concurrents.
De 2016 à aujourd'hui	Utilisation de Dapp : sur Ethereum d'abord, sur de nombreux autres protocoles ensuite	Ethereum, mais aussi Polygon, Cosmos et son écosystème, Solona, les solutions de seconde couche d'Ethereum (comme Optimism, Arbitrum, ZksyncEra, etc.) Hors chaîne* : exploration continue de la diversité des usages émergents (financiers ou non). Au sein du protocole* : exploration continue de la diversité des usages émergents (financiers ou non).	Utilisation de DApps (applications décentralisées), notamment Ethereum, ses protocoles de seconde couche (cf. Optimism, Arbitrum, ZksyncEra, etc) et les protocoles de L1 concurrents (cf. Polygon, Cosmos, Solana etc.) ; exploration continue de la diversité des usages émergents, qu'ils soient financiers (DeFi) ou non (NFT, jeux, réseaux* sociaux, etc). Des usages financiers d'abord avec les protocole et services de DEFI : trading de CM et crypto-actifs* *on chain* via* différents type de DEX avec plus ou moins de fonctionnalités (à découvert ou non, type d'ordres, etc.) ; market making *via* provision de liquidité dans des DEX (Decentralized Exchange), tels que Uniswap, qui permettent de faire des transactions* directement sur la blockchain, sans intermédiaire ; nous avons bénéficié d'Airdrop et participé à la campagne de liquidity mining, qui consiste à recevoir des tokens gratuits ou à les gagner en échange de la fourniture de liquidité à des DApps ; nous avons réalisé des dépôts rémunérés (Aave, Compound, etc.) et des demandes de crédit en stable coin, garanties par nos CM mises en séquestre comme garantie en utilisant des protocoles de prêt, tels que MakerDAO ou QiDAO; achat et fourniture de produits d'assurance, qui permettent de se couvrir contre les risques liés aux DApps, tels que les bugs, les hacks, les pertes de fonds, etc., en utilisant des protocoles d'assurance, tels que la coopérative Nexus Mutual dont nous somme membre : nous avons pris part à la fourniture d'assurance, et subi les pertes liées au

			paiement des couvertures, bénéficié nous-même de paiement de couverture et voté à la gouvernance. Des usages non financiers ensuite, avec notre participation : à des réseaux* sociaux distribués (cf. Steemit, Lensprotocol, Farcaster, FriendTech) ; à des protocoles d'identité/réputation décentralisés (Proof of Humanity ; Degenscore ; Gitcoin passeport, etc.) ; à des jeux mêlant plus ou moins directement de la DEFI (cf. Aavegotchi, Age of Gods) ; à la collection des NFT *via* le marché primaire (les mint d'artistes ou de projets) ou le marché secondaire (achat/vente sur place de marchés comme Opensea, Blur) ; à un protocole de dispute décentralisé comme juré tiré au sort (cf. Kléros), etc. Appréhension des aspects techniques, économiques, sociaux, etc. des DApps et des protocoles de CM : interaction utilisant des portefeuilles*, des navigateurs, des extensions, etc. compatibles avec les réseaux* blockchain considérés; confrontation aux opportunités et aux risques liés à de tels services : notons que, comme tout usager, des pertes ont été encourues, qu'elles soient liées à de mauvaises utilisations (cf. erreur d'envoi, perte de clef cryptographique de hotwallet de faible valeur), à des attaques/effondrement de plateformes (Terra Luna, *via* son stablecoin UST, majoritairement utilisé dans l'écosystème Cosmos) ou des attaques personnelles (si de nombreuses tentatives ont été subies, aucune perte de fonds ou de NFT n'est à déplorer ici).

Annexe IV.2 : Détails des observations participantes

	Date Lieu	Type d'événement	Nom de l'événement et Thématique(s)	Temps (Heure)
	15-10-2016 Paris	*Meet Up* Asseth	Lancement de l'association Asseth et débriefing DEVCON2	3
	10-12-2016 Paris	*Meet Up* Asseth	Atelier monnaies locales et tokens sur Ethereum	2
	02-11-2016 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	3
	17-11-2016 Paris	*Meet Up* Bitcoin-Paris	Inauguration du "Bitcoin Boulevard" à Paris (Passage du Grand Cerf)	2
	29-11-2016 Paris	Meetup Chaintech	Découvrez des projets Blockchains concrets ! (Consilium; DACA; Iex.ec; Beyond The Void; Kidner Project; Woleet; IOTA)	3
	01-12-2016 Paris	*Meet Up* Bitcoin-Paris	Présentation de Bitsquare avec la "Team" de Barcelone	2
	01-02-2017 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
	01-03-2017 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
	05-04-2017 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2

0	18-04-2017 Paris	*Meet Up* Asseth	3 présentions autour du web 3.0 et du stockage décentralisé	2
1	03-05-2017 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
2	30-05-2017 Paris	Conférence Bitcoin	Bitcoin Paribus Impar Programme : https://bitcoin.fr/bitcoin-pluribus-impar-3/	4
3	29-06-2017 Paris	*Meet Up* Asseth	Meetup Identité décentralisée	2
4	09 et 10-09-2017 Paris	Conférence Bitcoin	Breaking Bitcoin 2017 Programme : https://breaking-bitcoin.com/otherPages/2017/2017.html	6
5	20-09-2017 Paris	*Meet Up* Asseth	Blockchain for Finance Présentation de VaribL, NapoleonX et Airswap	2
6	04-10-2017 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
7	19-10-2017 Paris	Repas de L'association du Cercle du Coin	27ème Repas du Coin	2 .
8	10-03-2018 Paris	Conférence Ethereum	EthCC 2018	12
9	25-05-2018 Paris	*Meet Up* Asseth	Asseth reçoit Parity + Snips chez Talan Labs	2

0	06-06-2018 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
1	23-10-2018 Paris	Présentation d'ouvrage et discussion	Présentation et dédicace de l'ouvrage *Bitcoin Metamorphose* + discussion	2
2	21-02-2019 Conflans-Sainte-Honorine	Repas de L'association du Cercle du Coin	42ème Repas du Coin	3
3	Du 05 au 07-03-2019 Paris	Conférence Ethereum	EthCC 2019 Programme : https://ethcc.io/	24
4	03-04-2019 Paris	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	2
5	08 et 09-06-2019 Amsterdam	Conférence Bitcoin	Breaking Bitcoin 2019 Programme : https://breaking-bitcoin.com/	16
6	04-03-2020	*Meet Up* Bitcoin-Paris	Social Meetup of Sofbar	3
7	Du 03 au 05-03-2020	Conférence Ethereum	EthCC 3 2020 Programme : https://ethcc.io/	24
		(d'environ deux en Moyenne =)	total	124

Annexe IV.3 : Statut(s) et Rôle(s) couvert(s) par les acteurs de nos entretiens

Entretien n°	Les « développeurs* »		Les « opérateurs du traitement » et de la « vérification » des transactions*				Autres Services (marchands ou non)							Utilisateurs finaux
	Couche protocole	Couche applicative	"Pool de minage"	"Hash*eurs" (individuel & collectif)	Fabricants de machine (ASIC)	Nœuds* complets	Portefeuilles *	Conservation de fonds & paiement	Bourses d'échange	Services d'analyse de données	Média & événementiel	Conseil, formation et enseignement	Autres (app/Dapp, projets divers)	Utilisateurs (Utilisateurs, Investisseurs, traders)
	NON	OUI	NON	OUI	NON	OUI	NON	NON	NON	NON	NON	OUI	OUI	OUI
	NON	OUI	NON	OUI	NON	OUI	NON	NON	OUI	NON	NON	NON	OUI	OUI
	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	OUI	NON	NON	OUI	OUI
	NON	NON	NON	OUI	NON	OUI	NON	NON	NON	NON	OUI	OUI	OUI	OUI
	NON	NON	NON	NON	NON	OUI	NON	NON	NON	NON	OUI	NON	OUI	OUI
	NON	NON	NON	NON	NON	OUI	OUI	NON	NON	NON	NON	NON	OUI	OUI
	NON	NON	NON	NON	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
	NON	OUI	NON	NON	NON	OUI	OUI	NON	NON	NON	NON	NON	OUI	OUI
	NON	NON	NON	NON	NON	NON	NON	NON	NON	NON	NON	NON	OUI	OUI
0	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	NON	OUI	OUI	OUI
1	NON	NON	NON	NON	NON	OUI	NON	NON	OUI	NON	NON	OUI	OUI	OUI
2	NON	OUI	NON	OUI	NON	OUI	OUI	NON	NON	NON	NON	NON	OUI	OUI

3	NON	OUI	NON	OUI	NON	OUI	OUI	NON	NON	NON	NON	NON	OUI	OUI
4	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	OUI	OUI	OUI	OUI
5	OUI	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
6	NON	NON	NON	OUI	NON	OUI	NON	NON	NON	NON	OUI	OUI	OUI	OUI
7	NON	NON	NON	OUI	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
8	NON	NON	NON	OUI	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
9	NON	NON	NON	NON	NON	OUI	NON	NON	NON	NON	OUI	OUI	OUI	OUI
0	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	OUI	OUI	NON	OUI	OUI
1	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	OUI	NON	OUI	OUI
2	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
3	NON	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	OUI	OUI	OUI	OUI
4	NON	NON	NON	NON	NON	OUI	NON	NON	OUI	NON	NON	NON	OUI	OUI

5	NON	NON	NON	NON	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
6	OUI	OUI	NON	NON	NON	OUI	NON	NON	NON	NON	NON	NON	OUI	OUI
7	/	/	/	/	/	/	/	/	/	/	/	/	/	/
8	/	/	/	/	/	/	/	/	/	/	/	/	/	/

Annexe IV.4 : Liste des entretiens menés et notice biographique succincte des enquêtés

Réf.	Nom[487]	Éléments Biographiques : *Âge ; Formation ; Découverte des cryptomonnaies* ; Expérience avec Bitcoin et / ou Ethereum ; Activités dans l'écosystème ; Revenu annuel*	Communauté	Conditions & Matériaux	Date (Durée)
#1	Anon 1	34 ans ; Ingénieur Bac +5 ; Découvert Bitcoin en 2012, intéressé par la technique et surtout l'activité de minage qu'il réalisera brièvement (il nous précise qu'il continue à miner de l'Ether). Il va se regrouper avec d'autres pour former la communauté parisienne. Lance au début quelques projets sur son temps libre avant d'en faire son activité principale - en conseil, service et sécurité - après un plan social en 2017 dans l'entreprise qui l'employait. Revenu annuel : ~40 k.	Bitcoin	Face-à-face Enregistrement audio	13/02/2019 (150 min)
#2	Anon 2	43 ans ; Bac +5 dans le domaine de l'informatique médicale. Découvert Bitcoin en 2013, brève activité de minage avec sa GPU. Puis cherche à se reconvertir dans des projets Bitcoin, du fait de sa longue expérience dans le *langage de programmation** C++. Il va travailler sur différents petits projets Bitcoin avant de se retrouver à travailler, faute d'opportunités, dans le secteur du paiement Internet. Il travaille aujourd'hui dans le secteur des bourses et du trading de CM – ce qui l'a poussé à apprendre le langage de programmation* « Python », utilisé dans ce milieu - et il reconnaît regretter de ne pas utiliser les codes Bitcoin dans son activité. Rev. ann. 60k euros.	Bitcoin	Face-à-face Enregistrement audio	19/02/2019 (120 min)

[487] Voir l'encadré précaution d'écriture concernant les principes d'anonymisation que nous avons suivi.

#3	Anon 3	45 ans ; Bac +5 école d'ingénieur, spécialisation en génie logiciel ; S'il a entendu parler de Bitcoin dès 2011, ce n'est qu'en 2013, à l'occasion d'une flambée des cours et d'une couverture médiatique, qu'il va vraiment commencer à s'y intéresser. La perte de son emploi d'alors lui laisse le temps d'étudier le WP*, ce qui le décidera à creuser ce qu'il considère comme une innovation technologique là pour rester. De par ses compétences et intérêt, il travaille à différents projets tournés vers la préservation de la vie privée. Rev. ann. ~ 42K (variable, car travailleur indépendant).	Bitcoin	Face-à-face Enregistrement audio	19/02/2019 (45 min)
#4	Jérôme De Tychet	32 ans ; Master en Économie théorique et empirique (Bac +5) à Paris 1 et une Maîtrise en Gestion des Organisations et de la Performance à Paris Dauphine, ; Il a toujours été attiré par le Hardware, les jeux vidéo et la lecture du WP* de Bitcoin l'a beaucoup interpellé. Il commence par du minage GPU sur Bitcoin en 2013, puis en 2014 mine différentes cryptos avant de passer sur Ethereum dès son lancement. Il a d'abord travaillé comme économiste statisticien pour diverses organisations (Eurostat, Bercy, ministère des Affaires sociales) avant de se rediriger vers le secteur des cryptos. Co-fondateur de l'association française Ethereum France (ex-Asseth), dont il est encore président, il participe à l'organisation de *Meet Up* et de conférence sur l'écosystème Ethereum (ETHCC Paris).De 2017 à 2020, il va travailler chez « Consensys comme « Blockchain tech lead », puis il passe chez « Ledger » comme « Global Head of Client Success », avant de fonder, en octobre 2021, le jeu fondé sur la blockchain « Cometh ». Il est aussi, depuis 2020, professeur associé au Conservatoire National des Arts et Métiers. Rev. ann. 100k < annuel (beaucoup de variable) [~ 80% de son épargne en crypto; précise - d'un Million]	Ethereum	- 1er Face-à-face; prise de notes - 2ème Face-à-face Enregistrement Audio	21/02/2019 (30min) + 01/03/2019 (65 min)
#5	Marc Zeller (pseudonyme)	Âge : non indiqué ; Hypokhâgne, un peu de Droit et d'Économie à Paris 1, de Droit et de Philosophie à Saint Hyppolyte mais surtout autodidacte. Vient des milieux underground et militants (squat avec "Jeudi noir", producteur de musique) avant de découvrir Bitcoin, mais surtout Ethereum pour qui il a plus d'intérêt. Va en faire son activité principale à partir de 2014 : *Freelance*, analyste chez « La maison du Bitcoin » (auj. « Coinhouse »), co-fondateur de l'association AssEth (auj. Ethereum France), de « The Block Cafe » et « Integration Lead » chez « Aave » (Ethereum).	Ethereum	Face-à-face Prise de notes	22/02/2019 (80 min)
#6	Taylor Monahan	Âge : non indiqué ; Études "Film and Television" à la New York University ; En 2014-2015, elle se redirige vers le développement web (Front End) ; En août 2015 avec le lancement d'Ethereum, elle co-fonde le service de portefeuille MyEtherWallet qu'elle quitte, après des controverses avec l'autre co-fondateur, pour fonder son propre projet de portefeuille Mycrypto, dont elle est actuellement la CEO. Personnalité très impliquée dans l'écosystème Ethereum depuis son lancement (modératrice de forum Ethereum, aide aux utilisateurs particulièrement lors de l'événement The DAO).	Ethereum	Face-à-face Prise de notes	06/03/2019 (25 min)

#7	Jordi Baylina	Âge : non indiqué ; Études d'ingénieur en télécommunication et Bac+5 (MBA) en Business Administration à l'Université de Navarra. Développeur* depuis ses 12 ans, il découvre Bitcoin en 2014 et lit le WP* qu'il trouve très stimulant. Militant et activiste, il s'intéresse aux technologies de décentralisation et va réellement s'intéresser aux crypto *via* Ethereum dès son lancement. Ethereum lui permet, contrairement à Bitcoin, des usages plus sophistiqués. Il va devenir une personne influente, particulièrement pour le projet The DAO.	Ethereum	Face-à-face Enregistrement Audio	06/03/2019 (14 min)
#8	Nicolas Bacca	42 ans ; Ingénieur de l'ENSI CAEN, Bac +5. Travaille dans les années 2000 sur la carte à puce avant de créer différentes start-ups dans le domaine de la sécurisation de secret. En 2012, création de l'entreprise BTChip, autour d'une carte à puce de sécurisation physique de Bitcoin (*Hardware Wallet*). Rapprochement avec Joël Pobeda (Chronocoin), Eric Larchevêques et Thomas France (La maison du Bitcoin/Coinhouse), et co-fondation de l'entreprise Ledger, une des entreprises leaders dans le secteur des portefeuilles* physiques. Actuellement CTO de Ledger. Rev. ann. ~100k euros.	Bitcoin & Ethereum	Face-à-face Enregistrement Audio	15/03/2019 (45 min)
#9	Vlad Zamfir	30 ans ; Bac +3 en Mathématique à l'université de Guelph. Se décrit comme autodidacte (apprentissage des mathématiques très jeune avec son grand-père, sur les crypto beaucoup d'apprentissage en ligne). Travail en freelance comme consultant, analyste et chercheur dans les architectures distribuée (PoS). Découverte de Bitcoin en 2013. Chercheur à l'Ethereum Fondation depuis 2014, suivant sa rencontre avec V. Buterin, et travaille spécifiquement sur le passage d'Ethereum à la PoS. Personnalité vocale dans la communauté, il avait lors de The DAO des avis assez dissonants (avait prévu un HF avant même l'attaque). Il n'est pas capable de me donner son rev. ann., car il ne gère pas lui-même ses finances.	Ethereum	- 1er Face-à-face; prise de notes - 2ème Face-à-face; Enregistrement Audio	13/03/2019 (90 min) + 14/03/2019 (91 min)
#10	Anon 4	39 ans ; Après le Bac, a commencé à travailler dans l'informatique au bas de l'échelle de salaire. VAE Bac+ 4 ; 15 ans de travail salarié dans différentes entreprises en Administration système. Découvre Bitcoin sur les réseaux* sociaux en 2011. En train de créer une entreprise en lien avec Bitcoin. Dernier salaire annuel ~ 100K, aujourd'hui sans salaire.	Bitcoin	Face-à-face Enregistrement audio	04/04/2019 (120 min)

#11	Alexis Roussel	43 ans ; Études de droit : licence de l'Université d'Aix-Marseille, maîtrise à l'Université Panthéon Sorbonne et un DESS de « Droit public des nouvelles technologies » à l'Université de Paris X Nanterre (BAC+5). D'abord juriste spécialisé dans les nouvelles technologies, il va travailler 7 ans aux Nations-Unies pour la Cour Internationale de Justice, sur les questions de gouvernance électronique. En 2009, il s'implique en politique et devient président du jeune Parti Pirate Suisse, poste qu'il occupera pendant près de deux ans. Il déclare avoir découvert Bitcoin dès 2009-2010, de par son intérêt pour les nouvelles technologies et son réseau* social largement ouvert aux activistes numériques (des membres du Parti Pirate et des connaissances se revendiquant Cypherpunk). Dès fin 2013-début 2014, il co-fonde - avec Y. Honoré, G. Bochlser et R. Braud - la plateforme d'échange de cryptomonnaie* « SBEX », renommée « Bity ». Il en sera le CEO durant près de 6 ans, avant de devenir le président de son conseil d'administration. En 2020, il devient administrateur* et COO de l'entreprise « Nym Technologies SA », qui travaille au développement de nouvelles infrastructures préservant la vie privée. Lui et « Bity » jouèrent un rôle important dans les évènements entourant « The DAO Hack » : Bity a été partenaire de l'entreprise « Slock It » à ses débuts, ce qui a permis de résoudre les problématiques juridiques que l'équipe rencontrait en Allemagne ; après la survenue de l'attaque de « The DAO », M. Roussel va conseiller et aider l'équipe de développement comme les membres des « White Hackers » (WHG et RHG) à leur protection juridique. Il publiera également, *via* le blog de Bity, des informations sur le déroulé des évènements et sur la résolution de crise. Salaire non communiqué, mais déclare qu'il est dans la catégorie des cadres et professions intellectuelles supérieures, au vu des statuts des membres de son ménage : lui, dirigeant d'entreprises, et sa femme, avocate, tous deux ayant des salaires suisses.	Bitcoin & Ethereum	Face-à-face Enregistrement audio	15/05/2019 (102 min)
#12	Fabian Vogelsteller	37 ans ; Études en communication et média à l'université de Buffalo, Master en Beaux-Arts (bac+5), en design média et développement web, film, audio et design d'interface à l'Université Bauhaus-Universität Weimar. Il a d'abord exercé des activités de designeur web avant de travailler en *freelance* à partir de 2015 et, pour près de 4 ans, pour la Fondation Ethereum. Il participe au développement du navigateur Internet « Mist » - avec A. Van de Sande - qui permet d'interagir avec les Dapp* Ethereum -, du portefeuille Ethereum principal. On lui doit d'autres contributions notables dans l'écosystème Ethereum, comme le développement de la bibliothèque « web3.js », qui n'est autre que la bibliothèque JavaScript la plus utilisée sur Ethereum. Enfin, il est parfois qualifié de « père des ICO », ayant participé grandement au développement des standards ERC20 et ERC 725, permettant de faciliter le déploiement de token sur Ethereum. Aujourd'hui fondateur et "Chief Blockchain Architect" pour Lusko. De par ses activités, il a participé activement à la résolution de la crise « The DAO » et était proche du RWG à l'époque.	Ethereum	Vidéoconférence Enregistrement Audio	25/05/2019 (124 min)

#13	Alex Van de Sande	Âge : non indiqué ; Études de design graphique à l'Université d'État de Rio de Janeiro. Activités professionnelles de designer d'interface et d'architecture de l'information. Ayant travaillé en freelance pour la Fondation Ethereum pendant près de 6 ans (UX designer et conseil), il y a participé au développement du portefeuille / navigateur Internet « Mist » - avec Fabian Vogelsteller - qui permet d'interagir avec les Dapp* Ethereum directement via son navigateur Internet ; il est aussi co-fondateur d' « UniLogin » sur Ethereum - et travaille aujourd'hui pour « Balancer Labs », entreprise qui développe des services de « bourse d'échange décentralisée » sur Ethereum (il s'agit d'un protocole de « tenue de marché automatique », appelé aussi « AMM* ») sur. A participé à la résolution de la crise « The DAO » et était proche du RWG à l'époque.	Ethereum	Vidéoconférence Enregistrement Audio	04/06/2019 (120 min)
#14	Jimmy Song	Âge : non indiqué ; Licence de mathématique à l'Université du Michigan, des formations en mathématique et cryptographie*. Suite à la crise de 2008, il déclare s'être intéressé à la monnaie et à l'économie, à travers la lecture d'ouvrages économiques « libéraux » et/ou relevant de l'« école autrichienne ». D'abord développeur* informatique avant de se reconvertir dans Bitcoin à travers différentes start-up. En tant que développeur*, il a travaillé pour la firme « Monetas » où il a pris la tête de l'équipe en charge de l'intégration de Bitcoin, comme manager du développement pour la firme « Armory Technologies », qui développe un portefeuille, il a aussi réalisé quelques PR sur le répertoire Bitcoin Core (~15 commit), relatifs majoritairement à des procédures de test. Aussi, bien qu'il soit développeur*, il préfère se décrire comme formateur et éducateur Bitcoin, reconnaissant que ses compétences et son expérience sur les codes sources Bitcoin ne sont pas suffisantes pour qu'il prenne part plus activement à cette activité. Il est une personnalité reconnue et vocale dans la communauté Bitcoin, se qualifiant volontiers de « Bitcoin Maximalist » pourfendeur de « shitcoin », et porte différents statuts : il produit des billets de blog et des vidéos éducatives sur Bitcoin, est l'auteur du livre *Programming Bitcoin* paru chez O'Reilly, est chargé de cours à l'Université d'Austin au Texas, réalise du conseil, et est membre de Blockchain Capital.	Bitcoin	Vidéoconférence Enregistrement Audio	14/06/2019 (58 min)

#15	Matt Corallo	28 ans ; Obtention d'une Licence de Sciences Informatiques à l'Université de Caroline du Nord, à « Chapel Hill ». Il devient tôt, dès 2011, contributeur sur le répertoire logiciel Bitcoin alors qu'il n'a que 18 ans et va rapidement devenir, suivant son engagement, un des « Core développeurs* » du logiciel Bitcoin Core. En 2014, après avoir été brièvement ingénieur logiciel chez Google, il co-fonde - avec A. Back, P. Wuille, G. Maxwell, M. Friedenbach, J. Timon, A. Hilll, J. Wilkins, F. Hall, A. Fowler - l'entreprise canadienne « Blockstream », spécialisée dans le développement des technologies de Blockchain, les systèmes distribués et les technologies associées à Bitcoin (« Liquid Network », « Blockstream Satellite », « Blockstream explorer », etc.). En 2017, M. Corallo commence à travailler chez « Chaincode Labs » - firme spécialisée dans la recherche et le développement sur Bitcoin – et son contrat couvre en partie le financement de ses activités de « Core développeur* » Bitcoin. En 2019, il change d'équipe pour travailler comme ingénieur « open source » au sein de la firme « Square » - entreprise américaine spécialisée dans les services de paiement numérique créée par J. Dorsey, aussi CEO de Twitter – qui lui offre, là encore, un contrat couvrant ses activités volontaires de « Core développeur* ». Revenu annuel : « Assez pour vivre à New York, mais pas pour toucher un salaire de Wall Street :) ».	Bitcoin	Vidéoconférence Enregistrement Vidéo	18/06/2019 (120 min)
#16	Simon Polrot	35 ans ; Études de droit à l'Université Paris 1 (Bac +5), École de Formation professionnelle des Barreaux de la Cour d'Appel de Paris. D'abord avocat fiscaliste et conseil, avant de se reconvertir et de s'intéresser aux cryptomonnaies*, particulièrement Ethereum. Lance en 2017 le projet « VariabL » intégré à l'entreprise « Consensys » Paris, en 2018. Co-fondateur de l'Asseth et aujourd'hui président de l'Adan (Association visant à défendre les Actifs numériques en France).	Ethereum	Face-à-face Enregistrement Audio	27/06/2019 (100 min)
#17	Sébastien Gouspillou	50 ans ; Maîtrise de marketing et de management à l'Institut Supérieur des Cadres Supérieurs de la Vente (ISCV-CNAM, Bac +4). Il a d'abord travaillé dans le commerce international, particulièrement avec l'Asie où il était spécialisé dans les produits financiers agroforestiers. Il découvre Bitcoin vers 2013, grâce à son ami informaticien Jean-François Augusti, et dit débuter sa réflexion sur l'économie et la monnaie. Mais c'est en 2015, suite à sa rencontre avec Robert Corby, un « mineur » américain développant alors des fermes en Ukraine, qu'il achète son premier mineur ASIC qu'il met en opération dans la ferme de Corby. Cette rencontre est pour lui un « élément déclencheur », qui le voit, début 2016, avec des amis français, lancer sa propre ferme de minage, hébergée alors dans les locaux de Corby. Pour ne pas porter seul les investissements initiaux importants, il développe un modèle de ferme, où les machines qu'il héberge et opèrent appartiennent à ses clients, qui lui donnent en gestion. En 2017, il co-fonde, avec J-F Augusti, l'entreprise « BigBlock Datacenter » sur le même modèle ; ils créent leur première « mine » en France qui, suivant la survenue d'une phase baissière importante du cours du bitcoin, ne s'avère pas rentable. Ils délocalisent alors leur ferme chez un « confrère » à Irkoutsk, en Sibérie et développent des fermes au Kazakhstan et en Azerbaïdjan. S. Gouspillou, *via* l'entreprise « BigBlock Datacenter », est aujourd'hui un des principaux acteurs de la filière du minage en France et de son expertise, il intervient dans les médias pour promouvoir ce secteur d'activité	Bitcoin	Vidéoconférence Enregistrement Vidéo	06/11/2019 (56 min)

		et répondre aux nombreuses critiques auxquelles ce secteur fait face.			
#18	Jean-François Augusti	50 ans ; Études d'ingénieur en informatique et système d'information à l'Université de Nantes et au Conservatoire National des Arts et Métiers. Il a travaillé en tant qu'administrateur* réseau* et système pour l'entreprise Servier, comme chef de projet chez BNP Parisbas, et travaille encore à son propre compte en tant que consultant en informatique. Il dit avoir découvert Bitcoin en deux étapes. D'abord, vers 2013 *via* un ami informaticien avec lequel il commence par découvrir le minage de Bitcoin (les premières UCN* gagnées n'ayant jamais été récupérées). Puis en 2017, S. Gouspillou est revenu vers lui pour lui parler de Bitcoin et c'est de là qu'il dit avoir vraiment commencé à s'y intéresser, particulièrement intéressé et « impressionné » par ses aspects techniques et sécuritaires. Ils co-fondent ensemble l'entreprise « BigBlock Datacenter », intervenant dans le secteur du minage, pour laquelle M Augusti est en charge des dimensions techniques en tant que CTO. Revenu annuel ~50K en tant dirigeant de société.	Bitcoin	Vidéoconférence Enregistrement Audio	13/11/2020 (40 min)
#19	Morgan Phuc	35 ans ; Études dans les mathématiques et la mécanique des fluides. Destiné à être ingénieur, il se met à jouer au poker afin de financer ses études et devient joueur professionnel pendant près de 11 ans. Il découvre Bitcoin et les « cryptos » fin 2011 *via* un camarade de promotion, Benoist Huget. Fin 2014, avec B. Huget et son frère, il co-fonde la start-up et le média « Bitconseil », qui produit des articles et ressources pratiques relatives à l'écosystème crypto en direction des lecteurs francophones. Il reconnaît s'être aussi intéressé à Bitcoin du fait de son côté militant, et se déclare lui-même proche de pensées « libertariennes ». En 2017, M. Phuc et B. Huget développent une activité de formation, dont ils ont la charge. En 2018, ils rencontrent et associent à « Bitconseil » les deux co-fondateurs du *Journal Du Coin*, un média au positionnement similaire qu'ils décident par la suite de développer plus fortement. La start-up « BitConseil/Journal du Coin », qui intervient dans le secteur des médias, du conseil, de la formation et de l'événementiel, dispose aujourd'hui d'une équipe d'une quinzaine de personnes et M. Phuc y est directeur du contenu et rédacteur en chef, formateur et, plus sporadiquement qu'avant, rédacteur d'articles sur les CM et crypto-actifs*.	Bitcoin & Ethereum	Vidéoconférence Enregistrement Vidéo	30/01/2020 (127 min)

#20	Antoine Le Calvez	26 ans ; Études en génie informatique, spécialité analyse de données, à l'Université de Technologie de Compiègne (Bac+5). Il découvre Bitcoin et les « cryptos » début 2013, durant ses études. Son intérêt est directement aiguillé par son intérêt et ses compétences pour l'analyse de données, qui lui sont directement accessibles, puisque ces systèmes financiers sont « ouverts » et « libres d'accès ». Il commence son activité d'analyse de données *au sein de la chaine** sur Bitcoin, avec la publication d'un site d'information intitulé « P2SH.info » (aujourd'hui txstats.com en collaboration avec « Bitmex Research » et « Coinmetrics », dont M. Le Calvez est salarié), qui dénombrait les transactions* Bitcoin utilisant le format de transaction* « Pay to Script Hash* ». C'est cette réalisation qui le fera connaître, ce qui va lui permettre d'entrer en contact avec des entreprises du secteur intéressées par ses compétences. Ainsi, en 2016, il réalisera son stage de fin d'études à Londres, à « Blockchain.info » – l'un des plus gros fournisseurs de services de portefeuille en ligne –, entreprise qu'il quittera en 2018 pour rejoindre l'équipe de « Coinmetrics ». Il travaille toujours aujourd'hui pour cette entreprise au sein de laquelle il est « Lead Blockchain Data Engineers ».	Bitcoin & Ethereum	Vidéoconférence Enregistrement Vidéo	06/02/2020 (69min)
#21	Léa Thiebaut	27 ans ; Études d'ingénieur « agronome environnementaliste » à l'Institut Supérieur d'Agriculture de Lille (niveau Bac +5). A travaillé un an dans les objets connectés en agriculture de précision avant sa découverte de Bitcoin fin 2014 et sa reconversion dans ce secteur. Co-organisatrice des conférences Breaking Bitcoin avec Pierre Lorcery et Kevin Loaec. Organisatrice de *Meet Up* Bitcoin à Neuchâtel. Elle a depuis pris ses distances avec l'écosystème et entamé une formation vétérinaire.	Bitcoin	Vidéoconférence Enregistrement Audio	12-02-2020 (110 min)
#22	Clément Lesaege	Âge : non indiqué ; Études d'ingénieur informatique, double diplôme de Master en Science de l'informatique, l'un à l'Université Technologique de Compiègne et l'autre à Georgia Tech (bac+5) ; Intéressé par les « cryptos » dès 2013 avec Bitcoin avant même le lancement d'Ethereum. Va d'abord jouer avec les Smart contracts* sur Bitcoin (les portefeuilles* multi-signatures), avant de découvrir l'ambition d'Ethereum de faire du SC beaucoup plus complexe et facile. Depuis 2016, travaille à plein temps dans le secteur, d'abord comme freelance dans la sécurité des Smart contracts*, puis à partir de 2017 comme CTO de Kleros (plateforme sur Ethereum financer *via* ICO). A acheté un peu d'Ether pour commencer à "jouer" avec Ethereum dès le lancement. A investi dans « The DAO », car le projet lui semblait intéressant. Reconnu dans l'audit et la sécurité des Smart contracts*.	Ethereum	Vidéoconférence Enregistrement Vidéo	13-02-2020 (80 min)

#23	Stéphane Roche	34 ans ; Études d'histoire et d'archéologie (double licence) à l'Université de Toulouse-le-Mirail, Master professionnel de "Documentaliste audiovisuel" à l'université de Paris Est Créteil (niveau Bac+ 5) et obtention d'un certificat professionnel en « Developpement Web » au Conservatoire National des Arts et Métiers. Découvre Bitcoin en 2014 pendant sa formation au Cnam, ce qui l'amène à réaliser, en 2015, un stage de fin d'études de six mois chez « Ledger » - une des entreprises leaders dans le secteur des portefeuilles* physiques. Après cette « première introduction » à Bitcoin, il va travailler près d'un an et demi sur Ethereum, avant de revenir à Bitcoin dont il se sent plus proche des valeurs communautaires. Il dit s'être éloigné d'Ethereum du fait de l'apparition des « ICO », des « scams » et du « bullshit », préférant la communauté Bitcoin qu'il décrit comme plus ancienne, technique et avec laquelle il partagerait la philosophie crypto anarchiste, la revendication « d'être souverain de son argent ». Il a été co-fondateur de l'association « Asseth », et il travaille depuis 2018 à Lisbonne – à « The Block Cafe » -, exclusivement sur Bitcoin. Il a monté une micro-entreprise, « Bitcoin Studio », avec laquelle il propose du développement et de la formation autour de Bitcoin. Cela génère peu d'activité, et il est actuellement en recherche d'emploi. Revenu annuel : « très faible » (~5000 euros), il « vit sur [s]es bitcoins depuis longtemps », dont une partie a été reçue de son activité chez Ledger, bien qu'il ait de temps en temps de courtes missions à « quelques milliers d'euros ».	Bitcoin & Ethereum	Vidéoconférence Enregistrement Vidéo	14-02-2020 (55 min)
#24	Pierre Noizat	Âge : non indiqué ; Formation d'ingénieur à l'école polytechnique suivie de l'obtention d'un Master à l'université Telecom ParisTech (spécialisation Telecom, niveau BAC +5) et réalisation d'un MBA en « Marketing et finance » à l'université de Colombia (NY). C'est de sa présence aux États-Unis et sa spécialisation en Telecom qui va le rapprocher de la cryptographie*, puisqu'il va travailler à l'époque pour une entreprise de télévision à péage (« directTV »). Il découvre Bitcoin et y « adhère » très tôt (dès son lancement), puisque ces activités lui permettent de travailler avec des cryptographes de haut niveau, comme d'être en mode veille technologique pour ce qui a trait à la cryptographie*. D'ailleurs, il souligne qu'il était déjà intéressé par les questions monétaires du fait d'amis intéressés par les monnaies alternatives. Dès 2011, il fonde – avec un associé – la première place de marché Bitcoin euro au monde : « Paymium.com », qui compte près de 15 salariés aujourd'hui. En 2018, il co-fonde la place de marché « Blockchain.io », offrant un plus large choix de cryptomonnaies* et crypto-actifs*. Revenu annuel : ~ 60 000 euros, il se « paye 5000 euros bruts /mois », considérant que se payer plus dans cet écosystème n'est pas très cohérent et que se « payer plus ne serait pas en lien avec l'économie de cet écosystème ».	Bitcoin & Ethereum	Vidéoconférence Enregistrement Vidéo	14-02-2020 (80 min)

#25	Hervé Hababou	44 ans ; Diplôme d'ingénieur informatique de l'ENSIIE – École Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise - Lisieux, complétée de formations professionnelles à la *London Business School.* Plus de 22 ans d'expérience dans l'informatique, où il tient différents postes (développeur*, commercial, chef de projet, directeur d'entreprise), le conduisant à être aujourd'hui chef d'entreprise et investisseur. Découvre Bitcoin assez tôt (la date n'est pas précisée) grâce à son ami Vidal Chriqui, avec qui il partage un intérêt pour la « *partie technique* ». Cet intérêt joint ses « *deux passions* » pour « *l'informatique et l'économie* », et le constat que « *des entreprises voulaient se financer pour travailler sur Bitcoin* », le poussera à « creuser » en tant qu'investisseur et entrepreneur. Comme investisseur, il se penche « *sur les entreprises et les business modèles qui allaient éclore* » de cet écosystème et, de « *fil en aiguille,* [il a] *investi à la fois* […] *dans Ethereum au tout début, et dans des entreprises qui travaillaient soit sur Bitcoin, soit sur Ethereum* ». En tant qu'entrepreneur, il lance avec Vidal Chriqui fin 2018 la start-up « BTU Protocol » : ambitionnant de développer des solutions de distribution utilisant le protocole de registre* distribué ; le protocole est lancé à la faveur d'une ICO sur Ethereum (finalisée début octobre 2018, elle récoltera pas moins de près de 5,5 millions de dollars à l'époque). Revenu annuel : relativement élevé, en tant que « *CSP++* », « *ça marche* » et il *« paye le plus à la cantine des enfants ».*	Ethereum	Vidéoconférence Enregistrement Vidéo	24-02-2020
#26	Bob Summerhill	Âge : non indiqué ; Études d'ingénieur informatique. Il rencontre V. Buterin en juin 2014, lors d'un repas à Vancouver (CA) organisé par son ami D. Lowi, et prend part au lancement d'Ethereum. De juillet 2015 et jusqu'à aujourd'hui, il travaille bénévolement pour la fondation Ethereum. Polyvalent, il participe à différentes activités : il travaillera sur le code source d'un client Ethereum en langage C++ (« *cpp-ethereum»*) dans l'équipe de C. Reitwiessner ; participera au développement de la première plateforme Ethereum finalisée, « Homestead » ; à la restauration du dépôt de cpp-ethereum-1.3.0 ("Homecoming") ; aux activités entourant le Fork* consécutif à l'attaque de « The DAO » ; à l'échec de la tentative d'octroi d'une nouvelle licence Apache 2.0 ; puis à la conférence DEVCON2 à Shanghai. Il a aussi travaillé pour le projet « Hyperlledger », une initiative open source à l'initiative d'entreprises régies par la Fondation Linux, visant à faire progresser la technologie blockchain. Il va aussi être engagé par Joe Lubin, de l'entreprise « Consensys », pour laquelle il travaille à la formation de l' « *Entreprise Ethereum Alliance* » (aujourd'hui le plus gros consortium sur les technologies de protocole de registre* distribué). Il va aussi créer l'entreprise « Sweetbridge ». Enfin, de janvier 2019 jusqu'à aujourd'hui, il est le directeur exécutif de l' « ETC Cooperative », dont l'objet est de conduire le développement du protocole Ethereum Classic et son écosystème et qui est née du conflit communautaire autour de la résolution par un hard Fork* de l'attaque de « The DAO ». Acteur « passerelle » refusant le « tribalisme », il travaille tant pour Ethereum que pour Ethereum Classic, et il est le seul acteur de la communauté Ethereum Classic qui ai accepté notre demande d'entretien.	Ethereum & Ethereum Classic	Face-à-face Enregistrement Vidéo	03-03-2020 (120 min)
#27	"Non-entretien"	Âge : non indiqué ; Formation : non indiquée ; Découverte des cryptomonnaies* : non indiquée ; Expérience avec Bitcoin et/ou Ethereum : développeur* Bitcoin Core à partir de 2014, il devient Core	Bitcoin	Échange mail &	02/2021

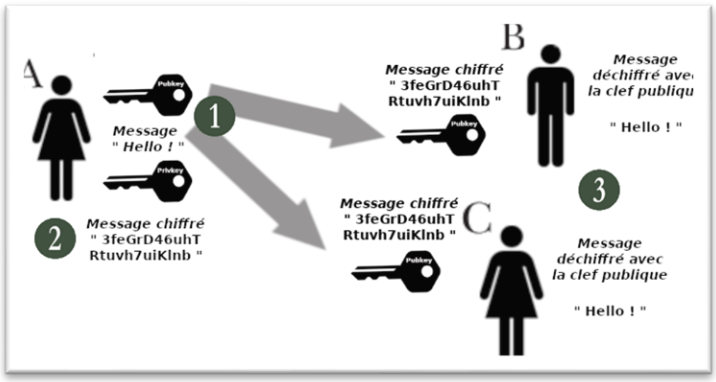
	avec Marco Falke	mainteneur en 2016, où il est en charge des tests ; il a aussi travaillé sur des outils de seconde couche, comme avec ses BIP 157/158, et on lui doit plus de 2 000 contributions au code source de Bitcoin Core. Pour ces activités, il a été financé par « Chaincode Labs » jusqu'en 2020, puis par « OKCoin » depuis 2021, et a annoncé son intention de quitter son rôle de mainteneur en 2023 (comme de nombreux autres Core mainteneurs) ; Revenu annuel : non indiqué. En l'absence d'entretien *stricto sensu*, les informations biographiques qui précèdent sont extraites de https://bitcoinmagazine.com/culture/marco-falke-bitcoin-network		*via* un Forum[488]	
/	SuperAnon	Correspond à un « acteur fictionnel » créé pour tenir le rôle de paravent, permettant de protéger l'anonymat d'acteurs, eux bien réels, que nous avons rencontrés. Si l'anonymisation totale a pu être demandée par certains, beaucoup des acteurs rencontrés ont accepté de le faire nommément. Reste que ces derniers ont pu nous demander explicitement que certaines des paroles qu'ils nous avaient données restent « en off », ne soient pas retranscrites ou tout du moins que leur origine ne soit pas dévoilée (avis / critiques privées, enjeux de réputation, information non publique, etc.). Aussi, nous leurs avons proposé une telle stratégie d'anonymisation : créer un personnage unique qui livrera l'ensemble de ces avis jugés controversés. À l'exception d'une information que l'on nous a livrée tout en nous précisant qu'elle ne pourrait en aucun cas être divulguée, même sous cette forme (impliquant un face-à-face, il aurait été possible à l'autre interlocuteur d'identifier cette source), les différents acteurs rencontrés ont ainsi accepté que de telles paroles soient portées par ce personnage.			

[488]Le forum « bitcoin.stackexchange.com »

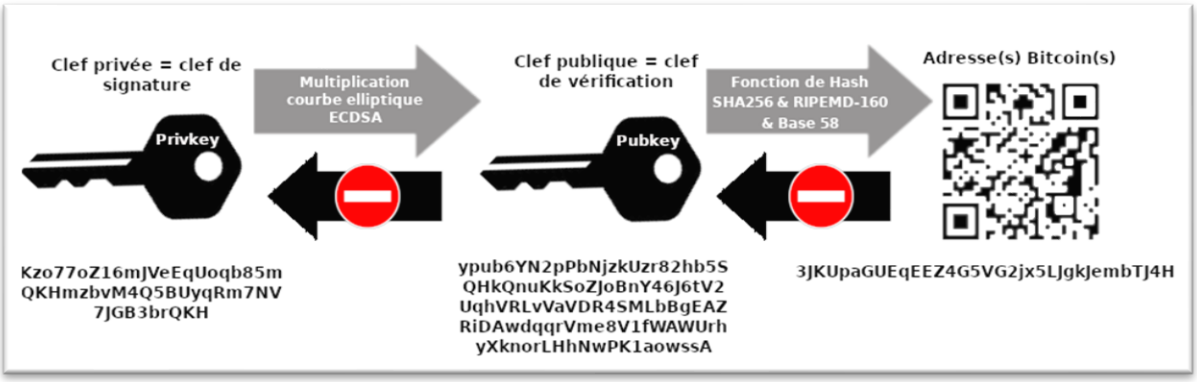
Annexe V: Retours circonstanciés sur les composants clefs et le fonctionnement d'une CM

Annexe V.1 : Cryptographie asymétrique et souveraineté individuelle

Le chiffrement asymétrique permet de réserver des informations aux seules personnes disposant des clefs adéquates, en garantissant une identification réciproque (Hughes 1993). Dans le schéma ci-contre, Alice (A) dispose d'un couple de clefs publique et privée. La première étape (1) est pour elle de partager sa clef publique. Dans un deuxième temps (2), elle chiffre un message ("Hello !") avec sa clef privée et transmet le message chiffré : "3feGrD46uhTRtuvh7uiKlnb" aux personnes B et C, qui peuvent (3) le déchiffrer grâce à la clef publique qui leur a été transmise. À l'inverse, B et C peuvent envoyer un message chiffré avec la clef publique de A, qu'ils connaissent, qu'elle seule pourra déchiffrer grâce à sa clef privée



Annexe V.2 : Clefs privées, clefs publiques et adresses Bitcoin



Le processus permettant de générer un couple de clés cryptographiques utilise une courbe elliptique, spécifiquement l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) pour Bitcoin. Cet algorithme dispose de procédures distinctes pour la signature et la vérification. La clé privée est utilisée pour signer les transactions*. La clé publique, dérivée de la clé privée *via* la courbe elliptique, est utilisée pour vérifier ces signatures. L'adresse Bitcoin est ensuite dérivée de la clé publique en appliquant les fonctions de hachage SHA-256 et RIPEMD-160, suivies du format d'encodage Base58Check pour faciliter l'utilisation et la vérification. Voir Rykwalder (2014).

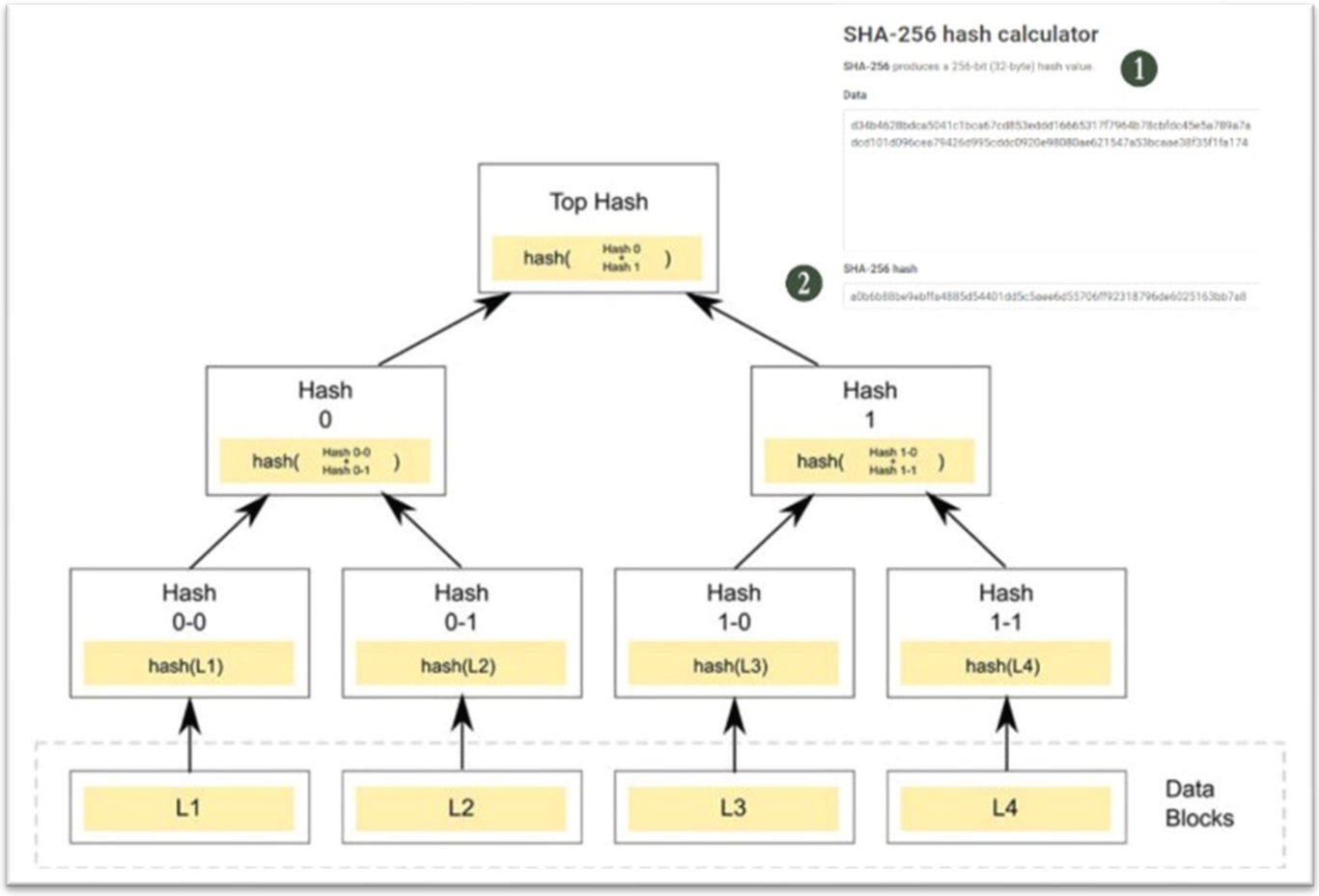
Annexe V.3 : La fonction de Hachage SHA 256

Une fonction de Hash*age est un algorithme cryptographique qui prend en entrée des données de taille variable et produit en sortie une donnée de longueur fixe, appelée « empreinte cryptographique »* ou « hash* ». Toute variation des données en entrée (ici, la présence ou l'absence de tréma sur le « e »), modifie les empreintes en sortie (2)[489]. Ainsi, toute personne disposant des données entrantes peut vérifier leur intégrité *via* le hash* transmis, qui doit correspondre à celui qu'elle réalise elle-même de son côté. Parmi les différents algorithmes de hash*age existants, Nakamoto a choisi pour les opérations de traitement des transactions* le SHA 256 (« Secure Hash*ing Algorithm 256 », utilisé dans notre exemple).

Annexe V.4 : L'arbre de Merkle

L'arbre de Merkle* renvoie à un usage particulier des fonctions de hachage qui permet à un ensemble de données, potentiellement très volumineux, d'être transformé tout en permettant de les retracer, en un hash* unique : le hash* sommet (ou « *Merkle root* »), dont il est possible de vérifier l'intégrité. Ce dispositif, proposé en 1980 par R. Merkle (pionnier de la cryptographie* asymétrique dont dérive le nom), visait à « *produire un condensé pour un répertoire public de certificats numériques* » de site Internet et les preuves numériques afférentes (Narayanan et Clark 2017, p. 8).

[489] Avec tréma, le *hash** est "d34b4628bdca5041c1bca67cd853eddd16665317f7964b78cbfdc45e5a789a7a" ; en son absence, il devient "dcd101d096cea79426d995cddc0920e98080ae621547a53bcaae38f35f1fa174".

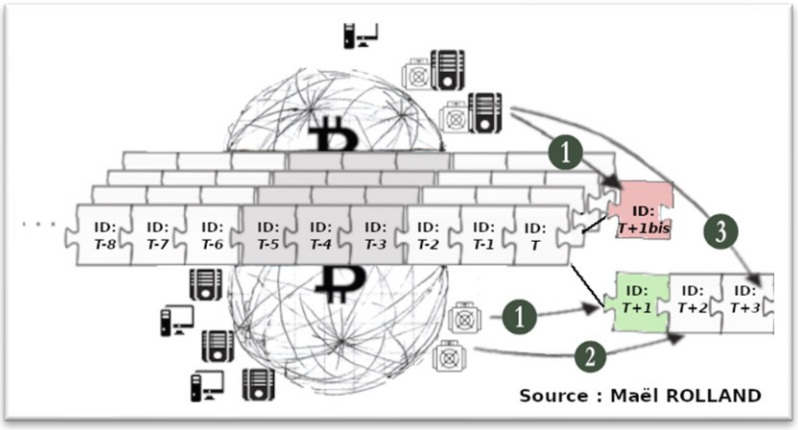


source : https://en.bitcoinwiki.org/wiki/Merkle_tree

Bitcoin utilise l'arbre de Merkel* dans la construction de chaque enregistrement sous la forme de bloc, où les feuilles sont des transactions*[490]. Une telle structure de données offrent des « *propriétés importantes* » : le hachage du dernier bloc – l'en-tête d'enregistrement* – est un condensé unique où toute modification de l'une des transactions* (« feuille ») modifie « *jusqu'à la racine du bloc et [les] racines de tous les blocs suivants* ». Ainsi, avec simplement la connaissance du dernier hachage valide, tout acteur peut « *télécharger le reste du grand livre depuis une source non fiable et vérifier qu'il n'a pas changé* » (*Ibid.*, p. 7). Dans le même sens, il est facile de « *prouver qu'une transaction* particulière est incluse dans le grand livre* » sans avoir à divulguer beaucoup d'informations (*Ibid.*). L'empreinte (2) est liée cryptographiquement aux empreintes des données initiales (pour nous (1)) et permet, en plus d'un gain important de taille, d'être facilement vérifiable.

[490] Dans l'exemple, les feuilles (Hash 0-0 et Hash 0-1) sont le *hash** de chacun des blocs de données initiales ("Thèse de Rolland Maël" et "Thèse de Rolland Mael") qui, concaténés deux à deux (1), permettent de calculer un *hash** parent Hash 0, ici (2) « a0b6b88be9ebffa4885d54401dd5c5aee6d55706ff92318796de6025163bb7a8 ».

Annexe V.5 : Cas d'une réorganisation malicieuse de type « Attaque 51% »



L'attaque 51% permettant une double dépense *off chain repose sur ce principe.**

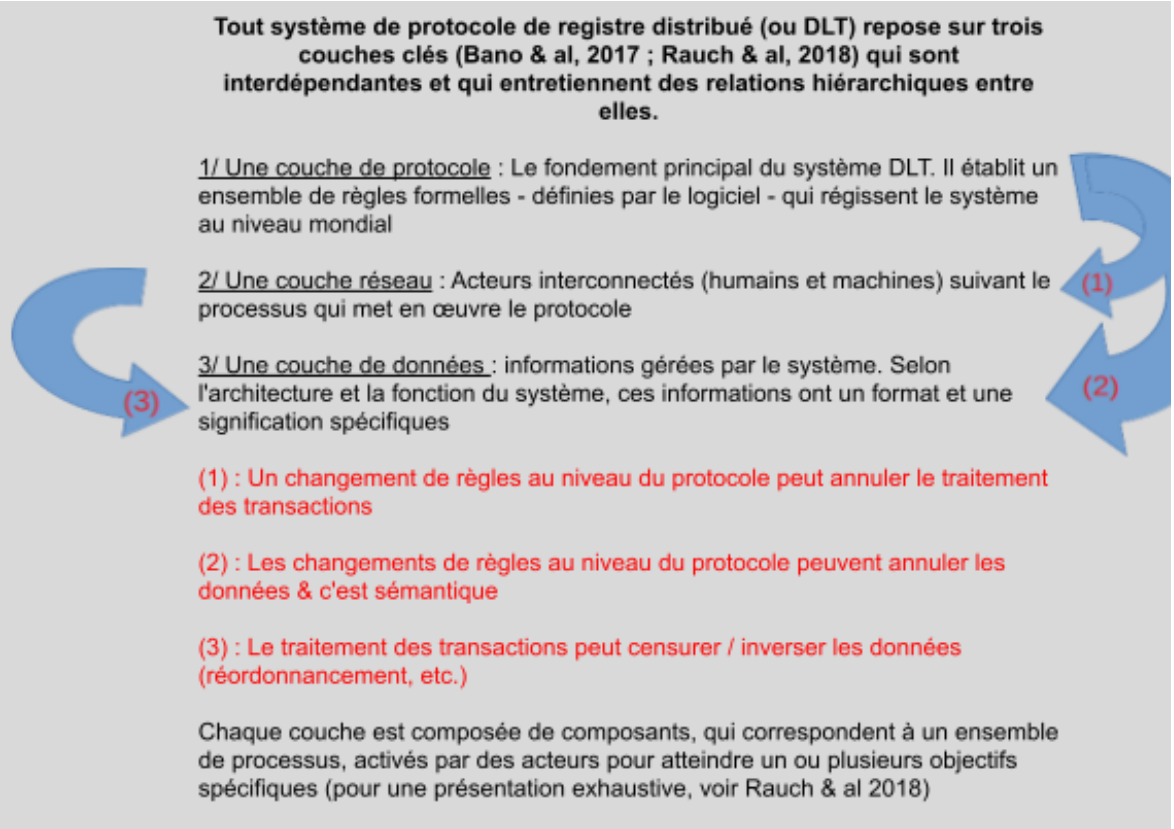
Si l'hypothèse de majorité des nœuds* honnêtes tombe, à un instant T, un attaquant est assuré de manière probabiliste de trouver les enregistrements plus rapidement que les autres nœuds*, ce qui lui permet d'imposer à terme sa version de l'HISTORIQUE DES TRANSACTIONS* contre une autre. L'attaque consiste à réaliser une double dépense dans le monde réel *via* une même UTXO* *on chain** : il s'agit d'un type particulier de double dépense (l'autre cas sera traité en Chapitre V) qui joue sur le principe de réorganisation précédent. Dans notre exemple, l'attaquant dispose d'une UTXO* de 10 BTC et **(1)** crée deux transactions* différentes la dépensant : l'une transfert les 10 BTC vers une plateforme d'échange et se trouve intégrée dans le bloc ***ID : T+1*** ; l'autre vers un portefeuille appartenant à l'attaquant, intégrée dans un bloc ***ID : T+1bis. Cet enregistrement candidat* valide a été produit par l'attaquant qui ne le diffuse pas au réseau*.*** Sur cette chaîne ***ID : T+1bis*** cachée de tous, l'attaquant continue d'ajouter des nouveaux enregistrements ***(ID : T+2bis, ID : T+3bis, ID : T+4bis, etc.***) : comme il dispose de plus de la moitié de la puissance de calcul, il est assuré que la construction de la chaîne ***ID : T+1*** sera, sur un temps donné, moins rapide et donc moins longue et lourde que la sienne. Conventionnellement, une plateforme d'échange va créditer le compte de l'attaquant après 6 enregistrements consécutifs (appelé "confirmation"), pour nous ***ID : T+6.*** Une fois crédités sur le compte de l'attaquant, les 10 BTC seront échangés contre d'autres actifs et retirés de la plateforme vers un portefeuille que l'attaquant possède. Pour l'heure, il dispose seulement d'actifs d'une valeur équivalente aux 10 BTC. Reste que, si les nœuds* honnêtes ont trouvé 6 nouveaux enregistrements (***ID : T+6***), l'attaquant lui, a déjà ajouté 8 enregistrements (***ID : T+8bis***) à la chaîne qu'il construit en secret. Une fois retirés les actifs achetés, il est temps de révéler à l'ensemble du réseau* la chaîne ***ID : T+8bis***. Dès réception de ce nouvel enregistrement, constituant une chaîne plus lourde relativement à la chaine « honnête », il devient canonique et tous les nœuds* convergent sur l'historique ***ID : T+1bis, ID : T+2bis, ID : T+3bis, ID : T+4bis, etc.***, annulant *de facto* toutes les transactions* qui avaient été traitées et enregistrées dans la chaîne ***ID : T+1, ID : T+2, …, ID : T+8bis.*** L'attaque est réalisée ! L'attaquant dispose donc de ses 10 BTC, qu'il s'est envoyé à lui-même *via* la transaction* inscrite dans l'enregistrement ***ID : T+1bis*** ET des actifs équivalents à 10 BTC qu'il a obtenus de la plateforme d'échange. C'est elle qui subit la double dépense et perd 10 BTC, puisque la transaction* première, inscrite en **ID : T+1**, n'a finalement jamais existé, et le compte de l'attaquant n'aurait pas dû être crédité. Les cas de doubles dépenses sur Bitcoin sont rares, mais pas impossibles[491] du fait de la grande puissance de calcul accumulée et de sa distribution, mais des cas de double dépense de ce type

[491] Voir par exemple https://twitter.com/BitMEXResearch/status/1221673450986565633

ont été rencontrés sur des CM moins sécurisées (voir, par exemple, le cas d'Ethereum Classic qui a connu des situations similaires à plusieurs reprises, forçant les bourses d'échange à allonger le nombre de confirmations qu'elles demandent (Voell 2020; Balakrishnan 2020).

La création monétaire s'opère à cette étape. L'enregistrement reconnu comme canonique contient la transaction* de récompense qui est traitée comme toutes les autres. Si l'opérateur victorieux peut directement dépenser les frais de transaction* payés par les utilisateurs (définis en (1)) qu'il a traités, ce n'est pas le cas des UCN* nouvellement émises. L'UTXO* créée par la transaction* *coinbase* a la particularité de ne pouvoir être dépensée qu'après que 100 enregistrements ont été produits au-dessus de celui qui la contient (Walker, Greg 2017). Il s'agit là d'une mesure de protection dans le cas où un bloc reconnu canonique un temps soit rendu orphelin, suite à une réorganisation de l'historique consécutive à un Fork* de chain. Malicieuses ou non, ces situations sont régulées par la compétition en PoW* - étape (2) – et la convergence se réalisera à terme *via* l'étape (3).

Annexe V.6 : Relations hiérarchiques entre les trois couches d'un protocole de registre distribué



Un système de protocole de registre* distribué correspond à l'articulation de 3 couches de clés interdépendantes et soumises à des relations hiérarchiques entre elle (les flèches bleues). La couche protocolaire est hiérarchiquement supérieure en ce qu'elle établit l'ensemble de règles formelles - définies par le logiciel - qui régissent le protocole et ce faisant, des changements de règles protocolaires peuvent (1) servir à annuler le traitement des transactions* ou (2) à annuler les données consignées et leur sémantique. On trouve un niveau

en dessous une couche réseau*, correspondant à un ensemble d'acteurs non humains interconnectés opérés par des opérateurs humains suivant le processus que met en œuvre le protocole. Cette couche est elle-même hiérarchiquement supérieure à la couche base de données où se trouve consigné l'ensemble des données endogènes* administrées par le protocole de registre, car ce sont ces opérateurs qui choisissent ou non de les consigner, et peuvent censurer / inverser les données (réordonnancement, etc.) qu'ils reçoivent.