

CHAPITRE III - AU-DELÀ DES CODES : LA GOUVERNANCE DISCRÈTE DES CM, DÉVOILÉE PAR LEURS CRISES

« Il y a trois époques pour la monnaie : la monnaie basée sur les matières premières, la monnaie basée sur la politique et, aujourd'hui, la monnaie basée sur les mathématiques. »

Chris Dixon (Co-Founder of Hunch and SiteAdvisor)

« Donc voilà, "don't trust verify", ben oui, il ne faut pas truster, il faut vérifier. "Code is law", là par contre au fur et à mesure du temps, au début j'étais dans ce côté-là, en effet : ben si le code dit cela, il va se passer cela. J'étais encore dans ce côté-là pendant la "CVE2018 je ne sais plus quoi là"... je me suis dit, ben finalement si quelqu'un avait exploité cela, est-ce que il aurait fallu accepter ou pas les changements, je me suis dit bon... il a fait ça, ok... Pareil avec "The Dao", avec le temps,...] je me dis qu'il y a quand même un consensus social. "Code is law", as long as people don't mind" [Il rigole]. »

A. Le Calvez, Entretien n°20

En 2018, « le monde du Bitcoin a été surpris » d'apprendre qu'un bogue critique nommé « Bitcoin CVE 2018 #17144 », venait d'être corrigé en secret (Song 2018; Bitcoin CVE 2018 ci-après). La surprise qu'évoque Song (2018) tenait au fait que le réel mettait ainsi à l'épreuve les prétentions monétaires libérales technicistes des *coiners** qui font de Bitcoin une monnaie naturellement saine et incorruptible car « régulée par un algorithme au lieu d'être régulée par des bureaucraties gouvernementales » (Antonopoulos cité par Kanev 2022). Une telle nouvelle avait de quoi ébranler ceux convaincus d'avoir « placé leur [...] argent et [leur] confiance dans un cadre mathématique exempt de politique et d'erreur humaine » (Tyler Winklevoss, cité par Mullin 2013). Pourtant, force est de constater que l'antienne des *coiners** les plus radicaux se heurte à la réalité et que, de fait, les CM ont réussi à traverser « une litanie de problèmes de sécurité [qui] alimentent régulièrement les gros titres des journaux » (*Ibid*), ce qu'une simple requête en ligne associant les mots « Bitcoin » / « Ethereum » et « vulnérabilité » permet de vérifier en produisant de milliers de résultats³²⁰.

Notre étonnement à nous renvoie plutôt à l'invisibilité relative des crises, à la fois pour les *coiners** et pour la plupart des académiques. A se demander « que se passerait-il si des circonstances imprévues comme une faille dans le code, une cyberattaque ou une instabilité systémique apparaissaient ? », impossible de conclure que « la communauté bitcoin ne semble pas s'en préoccuper car elle a foi dans bitcoin » (Ponsot 2021, p. 2), alors même que la crise Bitcoin CVE 2018 s'inscrit dans l'histoire longue de celles déjà traversées par Bitcoin et que sa gravité potentielle avait de quoi faire parler. La faille décelée permettait ce que Bitcoin est censé empêcher : l'émission d'UCN* en dehors des règles de monnayage canoniques via l'acceptation de transaction* de double dépense par des nœuds* du réseau*. Pour certains, il s'agit du « bogue Bitcoin le plus catastrophique jamais advenu » (Awemany 2018) et « l'une

320

Voir

<https://www.google.com/search?q=%C2%AB+Bitcoin+%C2%BB+et+%C2%AB+vulnerabilit%C3%A9+%C2%BB> et
<https://www.google.com/search?q=%C2%AB+Ethereum+%C2%BB+et+%C2%AB+vulnerabilit%C3%A9+%C2%BB#ip=1> [consultation au 04/07/2022].

des plus importantes failles de sécurité de [son] histoire » qui aurait pu en changer le cours même (Qtum 2020). Et il s'avère que cette crise n'est ni la première, ni la dernière : de 2009 à 2020, nous en avons recensé 38 (cf. Chronologie 4 section III.1.2). Cependant, la grande majorité n'était pas d'une telle gravité, et la faille Bitcoin CVE 2018, restée inactive et latente, n'éprouvera pas le monnayage de Bitcoin. Mais ce monnayage ne fût pas toujours épargné : ainsi, la crise dénommée « *Bitcoin bug Value Overflow* » de 2010 fut accompagnée de l'émission surnuméraire de près de 184 Milliards d'UCN* BTC, très loin du cap des 21 millions (Sedgwick 2019n). De même, peu de *bitcoiners** savent que ce cap pourtant annoncé par Nakamoto était mal codé à l'origine et ne fût réellement implémenté qu'au détour d'une nouvelle crise, en 2014. En revanche, les *coiners** savent par expérience que des controverses et conflits communautaires parfois houleux peuvent dégénérée en crise (cf. « *Scaling Debate* », Chap.I section I.3.3, Encadré 4 ; et la crise du hard Fork* d'Ethereum consécutif à l'attaque de « *The DAO* », ce chapitre).

Au fur et à mesure de nos recherches nous avons fini par trouver, au sein des groupes de *coiners** et chez les académiques, des personnes pour qui la survenue de crise n'avaient rien de surprenant.

Du côté des *coiners**, l'histoire des crises touchant à leur CM est souvent mal connue. Mais cette méconnaissance traduit les enjeux de visibilité et d'invisibilisation au cœur de tout phénomène de crise, et la forme particulière qu'elle prend dans le champ des CM. Rapportée aux slogans *coiners** « *Don't trust verify* », « *Be your own Bank* » ou « *trust no one* », cette méconnaissance des crises révèle qu'une partie d'entre eux se désintéresse des questions de sécurité et ce, en contradiction avec l'ethos annoncé revendiquant une souveraineté individuelle faite du refus de toute forme de confiance, de délégation et d'intermédiation. Les crises, loin de n'être que de simples accidents techniques renvoient à l'existence de risques réels ou perçus pour le protocole et ses participants, comme d'arrangements institutionnels et de stratégies développées pour s'y adapter. Elles mettent en lumière une division sociale du travail qui voit des membres formellement en charge d'administrer les codes et les crises qui y touchent : les « *Core développeurs** » du protocole considéré. De leur côté, ni surprise, ni alarmisme. Comme cela a été mis en évidence pour l'accident nucléaire de Fukushima, le statut de « *catastrophe inimaginable* » est suspendu à un processus de normalisation, dont certaines personnes (ici les Core Devs) sont les acteurs quotidiens : ces dernières réintègrent ces « *accidents* » dans l'ordre d'une normalité organisée, dont les modalités relèvent d'une « *politique de la crise* » qu'il faut interroger (Aguiton, Cabane et Cornilleau 2019, p. 17). La surprise des *bitcoiners** à l'annonce de la crise Bitcoin CVE 2018 se comprend à l'aune de cette politique de crise faite d'arrangements socio-technique négociés, liant normalisation et normalisateurs : si pour de nombreux *bitcoiners**, il est « *difficile de croire qu'un bug aussi critique* [que le bogue CVE 2018] *puisse se produire* [et qu'il soit] *passé inaperçu... pendant presque deux ans* », c'est qu'ils s'attendent à ce que de nombreuses « *relectures du code* [soient] *faites* » et que, dans le même temps, ce code soit exécuté par des logiciels clients, sur des machines et par des acteurs diversifiés, tenant des fonctions identiques (*Bitcoin Q&A* 2018). La « bonne » CM, celle en laquelle on a confiance, apparaît de ce fait moins fondée dans ses caractéristiques techniques faillibles (et « *les mathématiques* », cf. C. Dixon en exergue), que dans la capacité de la communauté et ses membres à faire face aux crises, des caractéristiques sociales et infrastructurelles. L'un des principaux enseignements de la crise Bitcoin CVE 2018 est que « *même la plus scrutée des cryptomonnaie* n'est pas exempte de bogue critique* » (Böhme et al. 2020, p.68). En conséquence, même la CM déclamée comme la plus *apolitique, neutre et immutable* des CM ne l'est pas, et suppose l'existence d'une gouvernance de crise.

Du côté des académiques, il existe quelques travaux qui, interrogeant la doxa qui prévaut d'une absence de gouvernance humaine des CM, en dévoilent *a contrario* l'« *invisible politique* » (De Filippi et Loveluck 2016). Citons par exemple (cf. Chap.II section I.3.3) Lustig et Nardi (2015, p. 1) qui, avec le concept d'« *autorité algorithmique* », démontrent que les *bitcoiners** reconnaissent la nécessité de la compléter par des jugements et médiations sociales, soulignant l'hétérogénéité des sphères axiologiques en présence, et donc potentiellement en conflit. Même type d'approche et de résultats pour DuPont (2018) qui s'intéresse à la communauté Ethereum durant la crise de « The DAO » (notre deuxième cas d'étude). Musiani, Mallard et Méadel (2018), quant à eux, étudient trois crises Bitcoin - l'une est protocolaire (le Bogues CVE-2013-3220, cf. crise n°19 Chronologie 4), les autres, infrastructurelles, concernent les affres de la bourse MtGox et de Silk Road (cf. Chap I). On doit à De Filippi et Loveluck (2016) d'avoir pointé que Bitcoin relevait d'une gouvernance duale, grâce à l'étude de la crise du « Scaling Debate » de Bitcoin : à la gouvernance *par l'infrastructure* (établie par les règles protocolaires), se superpose une gouvernance *sur l'infrastructure*, socio-économique et politique qui régule les codes logiciels et les propriétés de la CM. La crise du Scaling Debate n'ayant pas trouvé de résolution à l'époque de leur analyse, ils concluaient face au *statu quo* apparent, que la gouvernance *sur l'infrastructure* de Bitcoin serait incapable de tenir son rôle, c'est -à-dire de permettre la « *formation de consensus entre des individus mis par des intérêts politiques et commerciaux parfois divergents* », du fait d'« *une structure de pouvoir hautement technocratique* » au sommet de laquelle les « *Core Devs* » jouiraient de pouvoir exorbitant (De Filippi et Loveluck 2016, p. 12-13; cf. Chap II section II.3.3). Nos premières réflexions sur la gouvernance de Bitcoin (Rolland et Slim, 2017) trouvent également leur origine dans la controverse du Scaling Debate et dans les travaux de De Filippi et Loveluck (2016). Bien que leur cadre d'analyse soit pertinent, nous estimons qu'il nécessite d'être actualisé et précisé, ne serait-ce que parce qu'à l'époque où ils écrivent le scaling debate n'a pas encore connu sa résolution finale (cf. Chapitre II).

Nous définissons les crises comme des « événements » fabriqués et gouvernés comme tels, par des diagnostics d'acteurs qui contribuent « *à la « mise en crise » d'une situation donnée* » à travers un travail de qualification et des dispositifs techniques (Aguilon, Cabane et Cornilleau 2019, p. 11-12 et p.15). Afin d'éviter de juger en surplomb les objectifs et moyens de la gouvernance des CM, nous devons nous efforcer d'être « *impartial relativement aux arguments avancés par les uns et les autres* » et de ne « *privilégier aucun point de vue* » (Callon 1986, p. 8). Cette exigence nécessite aussi d'analyser « *la politique de la crise* » et « *son gouvernement* » d'un bout à l'autre, de la mise en crise à la remise en ordre : il convient d'interroger les conditions de sa « *survenue* », de sa « *normalisation* », de son « *aggravation* », de sa « *contention* », jusqu'à sa « *résolution* ». Dénaturaliser le phénomène de crise implique d'abandonner la recherche des causes et de se défaire de la distinction entre l'état routinier du monde et le phénomène critique. Il importe dès lors d'interroger les catégories mêmes qui opposent la routine au dysfonctionnement, le bogue à l'attaque, et le normal à l'exceptionnel (*Ibid.*, p.4). L'enjeu d'une crise, c'est d'abord la fixation d'un normal opposé à un pathologique. Les crises démontrent que ce n'est pas n'importe quel code qui peut être considéré comme la loi, alors même que le slogan « *code is law* » prive de sens les concepts de failles, de vulnérabilités, de bogues voire d'attaques, puisque tout résultat d'un code est réputé normal, indiscutable et légitime. Les *coiners** du camp de la règle radicalisée qui mobilisent ce slogan s'empêchent de reconnaître un écart problématique entre le produit désiré d'un code (son « *esprit* ») et le résultat obtenu de sa « *lettre* ».

Ce troisième chapitre resserre le propos de la thèse autour de la fabrique et de la gouvernance des crises de CM. Son enjeu principal consiste à documenter et analyser la gouvernance polycentrique que nous avons identifiée et présentée comme la caractéristique les

singularisant comme monnaie (cf. chap. II) à travers deux cas de crises différentes de CM – la crise Bitcoin CVE 2018 et la crise du *Hard Fork** d’Ethereum suite à l’attaque de « *The DAO* ». La crise Bitcoin CVE 2018 a été choisie pour le type de crise et de gouvernance qui s’y construit, d’apparence hautement centralisée et technocratique : relevant d’une vulnérabilité affectant le monnayage de Bitcoin corrigée « *dans les coulisses*, [sans que cela nécessite a priori que] tout le monde [soit] d’accord avec la direction que prennent les choses » [M. Corallo Entretien n°15], elle apparaît en contradiction avec l’idée d’une gouvernance polycentrique. La seconde crise, en revanche, émerge en dehors des codes du protocole d’Ethereum. Mais l’utilisation de ces codes comme moyens de remédiation – permettant d’annuler l’attaque du fonds d’investissement décentralisé « *The DAO* » et de restituer les fonds aux investisseurs volés – va conduire à une controverse communautaire intense. Nous avons choisi cette crise car elle partage avec le « *Scaling Debate* » le fait de revêtir les caractéristiques d’une controverse technologique à la Callon (2006, p. 5, cf. encadré n°4 Chap. II.3.3) et de conduire à un dénouement sous forme de schisme (ou *Fork**) du fait de la sécession d’une minorité en désaccord sur ce que doit être l’objet monétaire et donc, sur les modifications protocolaires désirables. Par ailleurs, cette crise de « *The DAO* » sur Ethereum a précédé le « *Scaling Debate* » de Bitcoin (qui ne fut donc pas pionnier) et a de fait établi un précédent. On peut la considérer comme fondatrice tant pour Ethereum que, plus largement, pour l’écosystème des CM, l’épisode du « *Scaling Debate* » en étant fortement imprégné.

L’analyse de ces crises permet de mieux saisir l’environnement matériel et idéal de la gouvernance des CM et de répondre à une série de questions les concernant : que recouvre une crise pour les *coiners**, en termes de diagnostic et de pathologies (réflétant les propriétés désirées ou non de la CM) ? Quels sont les nomenclatures, les catégories et critères de définition des crises de CM ? Qui sont les acteurs non humains défaillants ? Qui sont les acteurs humains, en charge d’établir diagnostics et parcours de soin ? Quels processus concourent à la mise en crise et à la remise en ordre ? Quels sont les dispositifs impliqués, à qui s’adressent-ils et à quoi servent-ils ? Comment se définit le consensus communautaire relativement aux modifications des codes protocolaires ? La gouvernance prend-elle une même forme relativement à une *crise liée à une vulnérabilité* et à une *crise liée à une volonté d’évolution* ? Comment ces crises révèlent-elles l’hétérogénéité et les conflits axiologiques présents dans les communautés de *coiners** ? Quelles institutions d’expression des accords ou désaccords structurent ces débats et conflits ? Quelles relations et dynamiques de gouvernance entre les différentes composantes des communautés de *coiners** se donnent à voir ?

Étudier des crises, c’est aussi l’occasion de réfuter l’ensemble des propositions du syllogisme « libéral-techniciste » des ambitions monétaires des *coiners** : très directement, en contestant précisément la proposition (iii) qui voudraient que les CM soient immunisées de la gouvernance humaine et de ses intérêts socio-politiques, et plus indirectement, en prouvant que la technique n’est pas autonome et neutre vis-à-vis du monde social (proposition [i]), que les CM ne sont pas des monnaies purement techniques (proposition [ii]) et qu’en faire de « meilleures » monnaies que les monnaies nationales, n’a que peu de sens (proposition [iv]) quand leur qualités attendues sont renégociées suivant l’existence de débats et de controverses endogènes à leur communauté de paiement.

Ce chapitre comporte trois sections. Les deux premières sont consacrées à l’analyse approfondie de Bitcoin et à notre cas de crise. Là encore, parce que Bitcoin est pionnier, les procédures, arrangements et dispositifs concourant à la fabrique et la gouvernance de ses crises servent de matériau génétique à ce qui est mis en place par les autres CM, comme Ethereum (d’où une présentation d’Ethereum qui fera l’économie des éléments déjà posés).

La **première section** (III.1), part d'une présentation périodisée de la crise Bitcoin CVE 2018, cernant à chaque étape les acteurs et arrangements impliqués. Cette crise sera ensuite replacée dans l'histoire des crises Bitcoin ce qui, en plus d'éclairer ses enjeux singuliers, offrira l'occasion de proposer un panorama de la diversité des crises que Bitcoin a déjà rencontrées.

La **deuxième section** (III.2) entend cartographier les acteurs qui participent de cette gouvernance - les logiciels clients et codes pris en défaut mais aussi les acteurs humains en charge de leur maintenance et de leur évolutions - ainsi que les dispositifs de régulation et de contrôle entourant ces activités critiques qui permettent à la communauté de se prémunir contre toute centralisation technocratique effective. De ce fait, nous distinguerons deux grands types de crise – les crises *vulnérabilité* et les crises *d'évolution* – ainsi qu'une gouvernance de crise des CM à deux faces : une face routinière, avec une gouvernance de *huis clos* où le consensus est tacite et local, comme dans le cas de la crise Bitcoin CVE 2018 et une face exceptionnelle, avec une gouvernance *publique*, où la production du consensus est large et manifeste, comme souvent conflictuelle.

Notre **troisième section** (III.3) vise à étudier spécifiquement cette face publique et conflictuelle de la gouvernance de CM à partir du cas de « The DAO ». C'est dans ces situations que s'éprouve de façon manifeste la réalité d'une gouvernance polycentrique où chaque frange de la communauté doit pouvoir décider du devenir de sa monnaie. Comme pour la crise Bitcoin CVE 2018, une présentation périodisée de la crise de « The DAO », permettra de réaliser une cartographie des acteurs et des dispositifs clefs à chaque étape des événements, d'expliciter ses enjeux conflictuels, tout en insistant sur les caractéristiques distinctives de cette forme de gouvernance publique en terme de production de consensus et de gestion des dissensus.

III.1 CRISE BITCOIN CVE 2018 #17144 : D'UNE CRISE À DE NOMBREUSES AUTRES...

La crise ouverte par la faille « Bitcoin Core CVE 2018 #17144 » (Bitcoin CVE 2018, ci-après) est singulière. Tout d'abord, parce que la vulnérabilité touche aux sacro-saintes règles de monnayage de Bitcoin. Ensuite, parce que cette vulnérabilité ne sera pas « activée », ni par exploitation volontaire, ni par occurrence fortuite (Bitcoin Core 2018a ; Böhme et al. 2020). Enfin, parce que le processus de découverte et de divulgation a permis une résolution silencieuse et confidentielle, grâce à un travail « *off chain** » coordonné par une poignée d'acteurs de confiance. Cette faille Bitcoin CVE 2018 doit sa découverte, le 17 septembre 2018, à « Awemany », un développeur « extérieur » à Bitcoin (Awemany 2018 ; Bitcoin Core 2018a). Ce dernier travaille sur la CM « Bitcoin Cash » (ticker BCH), née d'un schisme communautaire et protocolaire retentissant (un *hard Fork** contentieux, cf. section III.3.3 ce chapitre) marquant le dénouement du « Scaling Debate » en 2017 (cf. Chap. II section II.3.3). Bitcoin Cash, en reprenant une partie du code source de Bitcoin lors de son *Fork**, hérite également de ses vulnérabilités potentielles, comme le démontre cette faille découverte sur l'implémentation « Bitcoin ABC », au développement de laquelle participe Awemany et qui affecte aussi Bitcoin. Sa découverte n'est révélée qu'à un groupe restreint de personnes de confiance, dans le cadre

d'une procédure de « divulgation responsable »³²¹: d'abord à des membres de son équipe, ensuite à ceux d'équipes travaillant sur des implémentations de CM exposées à la même vulnérabilité (Awemany 2018). Dans ce cadre, le même jour, l'équipe « *Bitcoin Core* » reçoit confidentiellement un rapport de vulnérabilité anonyme concernant une faille par *Deni de Service* (DoS, Bitcoin Core 2018). M. Corallo, qui analyse ce rapport, découvre qu'il est partiel. La faille rapportée induit deux itérations de bogue, suivant les versions du client logiciel concernées : à celle ouvrant à des d'attaques par DOS identifiées par Awemany s'en ajoute une plus grave, permettant ce que Bitcoin est censé empêcher, à savoir la création monétaire *ex nihilo* d'UCN* en dehors du monnayage canonique, par acceptation de double dépense (Awemany 2018; Song 2018c).

Cette vulnérabilité et ses itérations différencieront sont complexes. Elles touchent aux processus de vérifications protocolaires entourant la double dépense. Leur introduction dans les codes est ancienne et ne s'est pas faite d'un seul coup : elle est le résultat de modifications et d'optimisations successives du code « *Bitcoin Core* » depuis son origine, et renseigne sur la dimension processuelle inhérente à la production et à la maintenance des codes logiciels Bitcoin. Il faut souligner le temps long pendant lequel la faille fut présente à l'état latent. Les versions vulnérables, toutes publiées en 2017, n'ont vu personne y prêter attention, de manière malicieuse³²² ou non (Bitcoin Core 2018a ; Song 2018) et il faut plus d'un an et demi à la communauté pour repérer et réparer le bogue. Oui, « *même la plus scrutée des cryptomonnaies* n'est pas exempte de bogue critique* » (Böhme et al. 2020, p.68). Catastrophique pour les uns (Awemany 2018 ; Qtum 2020) et à relativiser pour d'autres (Song, 2018), cette crise et sa gravité questionnent. Que « *ce bogue ait été introduit puis autorisé à exister de la 0.14.0 à la 0.16.2 a indéniablement été un échec majeur [et] si toutes les pratiques de Bitcoin Core restent les mêmes [...] nous pourrions ne pas avoir autant de chance [puisque] un échec similaire* » se reproduira nécessairement (theymos 2018). L'auteur reconnu de cette alarme enjoint justement à documenter ces « pratiques » entourant l'évolution des codes et les acteurs, ainsi que les procédures et dispositifs en place qui les encadrent.

Ces pratiques et l'ensemble de ce qui s'y rapporte, nous proposons de les faire ressortir à travers la périodisation des évènements entourant la crise CVE Bitcoin 2018.

III.1.1 Présentation périodisée de la crise Bitcoin CVE 2018

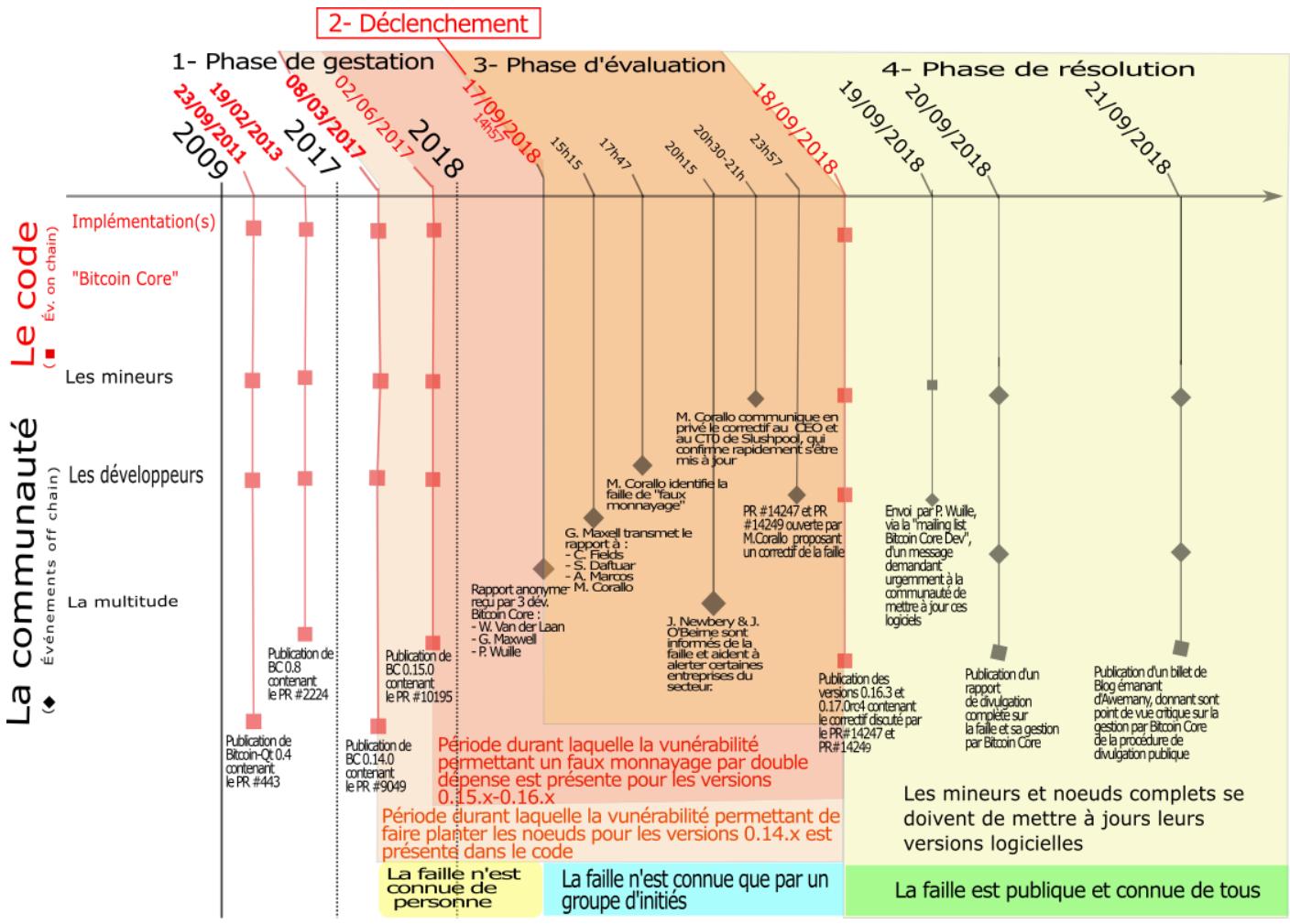
Comme nous le verrons, la faille étiquetée CVE 2018 #17144 n'est, pour Bitcoin et sa communauté, ni la première, ni sans doute la dernière (Cvllr 2018 ; Sedgwick 2019n ; Sedgwick 2020 ; Dashjr 2019)... ni même peut-être la plus intéressante en termes de sociologie des controverses technologiques au sens de Callon (2006, cf. section X). Mais pour s'en rendre

³²¹ Une procédure de « divulgation responsable » renvoie, dans le champ de la sécurité informatique, à un ensemble de conventions et de normes encadrant les pratiques de divulgation d'une vulnérabilité informatique : de sa découverte à sa divulgation publique, en passant par sa résolution. Ces procédures visent à préciser comment doivent être protégés les utilisateurs, qui doit être contacté, suivant quelle modalité et temporalité, et enfin, comment doit être récompensé le découvreur qui s'y est engagé. Ce type de procédure, normé au sein de l'industrie logicielle, reste largement informel, flou et problématique pour les CM et crypto-actifs* (Böhme et al. 2020).

³²² Lors de la divulgation complète du 21 septembre 2018, l'équipe « *Bitcoin Core* » reconnaît, sans plus de certitude, n'avoir « *pas connaissance de tentatives d'exploitation de cette vulnérabilité* » (Bitcoin Core 2018a) et il s'avère qu'*« une analyse rétrospective a prouvé qu'il n'a jamais été exploité ! »* (Straw Hat 2019).

compte, il importe d'abord de présenter cette crise et son contexte, à travers la réalisation d'une périodisation. Analyser un événement oblige à le borner temporellement, ce qui n'est jamais chose aisée – le réel étant continu et non discret. Le travail de périodisation est en soi un acte nominaliste, toujours relatif aux vues de son auteur, et notre périodisation ne fait pas exception. Puisque le « *statut de la crise est délicat à saisir et sa temporalité difficile à fixer* », nous adoptons « *une définition a priori [qui part du] diagnostic porté par* » des acteurs contribuant « *à la "mise en crise" d'une situation donnée [par un] travail de qualification* » suivant différentes opérations et dispositifs techniques (Aguiton, Cabane et Cornilleau 2019, p. 15). Cela nous permet de découper les événements en deux périodes et quatre phases (cf. Chronologie 3 suivante). Précisons que, pour la crise Bitcoin CVE 2018, ce bornage fut facilité par ces caractéristiques. La période de la mise en crise d'abord, constituée d'une phase d'insémination et de gestation au cours de laquelle la vulnérabilité est introduite dans le code, sans qu'elle ne soit ni activée, ni connue. Ensuite, une phase de déclenchement de crise, qui voit le statut de ce code changer, la faille passant de latente à manifeste. Pratiquement, cette mise en crise, conçue comme apparition consciente de l'existence d'une vulnérabilité, correspond à la première borne posée. Elle renvoie explicitement à la date de mise en œuvre de la procédure de divulgation responsable. C'est la fixation de cette borne qui permet, à rebours, de retracer les événements ayant pris part à l'émergence de la vulnérabilité, à sa découverte, à son évaluation et, enfin, à la production et à la publication du correctif. Nous faisons en amont débuter la phase de gestation en janvier 2009, car la faille, nous le verrons, s'articule aux premières règles protocolaires permettant de réguler les transactions* et le phénomène de *double dépense**. Le déclenchement, sous forme d'un rapport de divulgation anonyme et confidentiel, ouvre une période de remise en ordre décomposée, elle, en une phase d'évaluation (permettant aux acteurs informés d'évaluer la gravité du bogue et de discuter des voies de remédiation) et une phase de résolution au cours de laquelle une solution corrective est acceptée, implémentée dans une nouvelle version logicielle et publicisée (laissant aux acteurs du réseau* le choix de l'accepter en mettant ou non à jour leur machine). Là encore, la phase de résolution se trouvait bornée par la date de publication des versions correctives. La frise chronologique suivante saisit, pour chacune de ces phases, les principaux événements et acteurs.

Chronologie 3 : Périodisation des événements entourant la crise ouverte par le bogue CVE 2018



Une mise en crise longue et silencieuse

Retraçons l'origine de la faille en réalisant une généalogie partielle des codes sources Bitcoin.

Insémination/gestation : une « étrange confluence d'événements » potentiellement catastrophiques

La faille Bitcoin CVE 2018 est le résultat de modifications et d'optimisations successives du code source de l'implémentation « Bitcoin Core » depuis son origine. La comprendre impose de retracer les évolutions par sédimentation lente d'optimisations successives du code logiciel originel. L'ensemble de ces modifications – au nombre de 6 (cf. Figure 10 suivante) – prit la forme de « Pull Requests » (PR) acceptées et fusionnées, donnant lieu à la publication des versions vulnérables (le traitement de ces termes et des dispositifs auxquels ils renvoient est renvoyé à une section prochaine). Pour comprendre l'« étrange confluence d'événements » (Song 2018) qui conduira à l'introduction d'une faille d'une telle ampleur dans les codes protocolaires Bitcoin, il faut expliciter les objectifs et justifications qui ont présidé à ces PR et à leurs implémentations.

Le point de départ n'est autre que la première version du logiciel Bitcoin-QT (version 0.1, Nakamoto 2009c³²³), publiée par S. Nakamoto en février 2009 (Song 2018) et qui ne permet pas de se protéger de tous les cas de *double dépense* possibles. Dans le cadre normal de Bitcoin, il est par définition possible de produire et diffuser une transaction* contenant une double dépense. C'est la faire accepter par les nœuds* qui est logiquement impossible. Au sein de Bitcoin, les transactions* valides sont définies négativement : les transactions* produites et diffusées se voient appliquer des critères d'invalidité afin d'évaluer qu'elles sont « pathologiques » et, de ce fait, doivent être rejetées (un avertissement est même diffusé, cf. Chap. I, section I.1.3.). Mais l'encadrement pratique de la double dépense est complexe. Produire et diffuser une transaction* Bitcoin renvoie à quatre situations possibles, dessinant quatre cas « *pathologiques* » de double dépense (les cas A, B, C, D ; voir Tableau 2 suivant, Song, 2018).

Tableau 2 : Les quatre types de double dépense* idéal-typiques sur Bitcoin

		Origine des transactions*	
		Transaction* publique de portefeuille	Transaction* privée d'enregistrement
Nombre de transactions*	Transaction* Multiple	(A) Plusieurs transactions* au sein desquelles la/les même(s) UTXO* est/sont dépensée(s).	(B) Plusieurs blocs au sein desquels plusieurs transactions* dépensent la/les même(s) UTXO*.
	Transaction* Unique	(C) Une même transaction* au sein de laquelle la/les même(s) UTXO* est/sont dépensée(s) plusieurs fois	(D) Un seul bloc au sein duquel la/les même(s) UTXO* est/sont dépensée(s) plusieurs fois

Source : Rolland Maël

Deux types de transactions* de double dépense peuvent être produits. Tous d'abord, on peut créer plusieurs transactions* différentes dépensant la même UTXO*, c'est le plus connu (cas A). Il est aussi possible de créer une seule transaction* dépensant en entrée plusieurs fois la même UTXO* (cas B). Une fois produite, la transaction* doit être proposée à l'intégration au registre. Bitcoin dispose de deux procédures de publication : soit avec des *transactions publiques issues de portefeuilles** (« *mempool transaction** », cas C), soit il s'agit d'une *transaction privée intégrée directement dans un bloc* (« *block transaction** », cas D, Song 2018). Les premières servent souvent à illustrer le fonctionnement de Bitcoin (comme nous l'avons fait dans le Chapitre I) : partant du client portefeuille des usagers. Ces transactions* sont publiques de bout en bout, de leur consignation comme transaction* en attente dans les journaux locaux des « mineurs » (la « *mempool** »), jusqu'à leur traitement et leur intégration dans un enregistrement candidat*. Le second cas (les *transactions privées issues d'enregistrement*) est plus rarement explicité. Ce type de transaction* ne peut être produit que

³²³ Les codes sources sont accessible ici : <http://btc.yt/lxr/satoshi/source/src/main.cpp?v=0.10.0> [consultation au 12/09/2021].

par les opérateurs du traitement des transactions*, ce qui souligne leur différence structurelle d'avec les autres acteurs. En effet, l'attention donnée aux « *transactions* publiques, issues de portefeuille* » occulte le fait qu'une transaction* Bitcoin n'a pas à être diffusée publiquement *via* la « *mempool* » pour être traitée et intégrée dans un « *bloc* » : tout producteur d'enregistrement peut créer un service de diffusion privée « *off chain* »* afin d'intégrer les transactions* de ses clients souhaitant éviter la *mempool* : ces transactions*, n'étant publiques qu'une fois validées au sein d'un enregistrement candidat*, sont protégées des abus de type MEV (cf. Chap. I., section I.3.3). Bitcoin permet de réguler ces quatre cas suivant des règles strictes, renvoyant à des procédures de vérifications de non-conformité (des « *checks* ») encadrant chacun d'eux (Song 2018). Les doubles de dépenses de type A suivent la règle stipulant que la première transaction* intégrée dans un enregistrement canonique* invalide toute transaction* impliquant le/les UTXO* déjà dépensée(s). Idem pour les types B : le premier enregistrement candidat* à devenir canonique invalide tout enregistrement impliquant des transactions* avec la/les même(s) UTXO* déjà dépensée(s) qu'il contient. Les types C renvoient à un check établissant qu'une transaction* contenant plusieurs fois les mêmes UTXO* devra être considérée comme invalide. Le cas D, enfin, considère qu'un enregistrement candidat* contenant plusieurs fois la/les même(s) UTXO* sera considéré invalide, l'horodatage* faisant foi. Le caractère multiforme pris par la vulnérabilité Bitcoin CVE 2018 repose, nous le verrons, sur le traitement différencié des régulations du cas D, suivant les versions logicielles concernées (d'où la cellule grisée, Tableau 2, Bitcoin Core 2018 ; Song 2018).

Dans le logiciel originel de Nakamoto, la régulation des types de double dépense* n'est que partielle, poussant à des évolutions successives de son code (cf. Figure 9 suivante). En juillet 2011, expliquant que toute double dépense, qu'importe son origine, doit être invalide, le « Core Développeur » (« Core Dev » par la suite) M. Corallo propose la PR 443³²⁴. L'objectif est d'encadrer les cas de doubles dépenses issues de transaction* publique de portefeuille (le cas C), en introduisant une nouvelle vérification³²⁵ empêchant que ce type de transaction* « *soi[t] relay[é]* » (*Ibid.*). Avec cette PR - acceptée de tous les participants et implémentée dans la version Bitcoin Core 0.4 -, chacun des cas de double dépense possibles (A, B, C et D) est maintenant régulé, mais au prix d'une redondance pour les cas B et D, vérifiés deux fois³²⁶ (*Ibid.*). En janvier 2013, P. Wuille (aka « *Sipa* »), un autre « Core Dev », propose *via* la PR 2224 de transformer la vérification inutile en une vérification de corruption de système afin d'améliorer « *la façon dont les erreurs lors de la validation* des blocs et des transactions* sont propagées, affichées et traitées* » (P. Wuille³²⁷). La modification introduit que, en cas d'échec, le logiciel renvoie un « arrêt de programme » ("Assert") et non une simple erreur (Song, 2018). Cette PR 2224 donne lieu à la version Bitcoin Core 0.8.0. Les modifications présentées n'induisent encore aucune vulnérabilité. Ce sont celles qui suivront qui scelleront la crise en devenir.

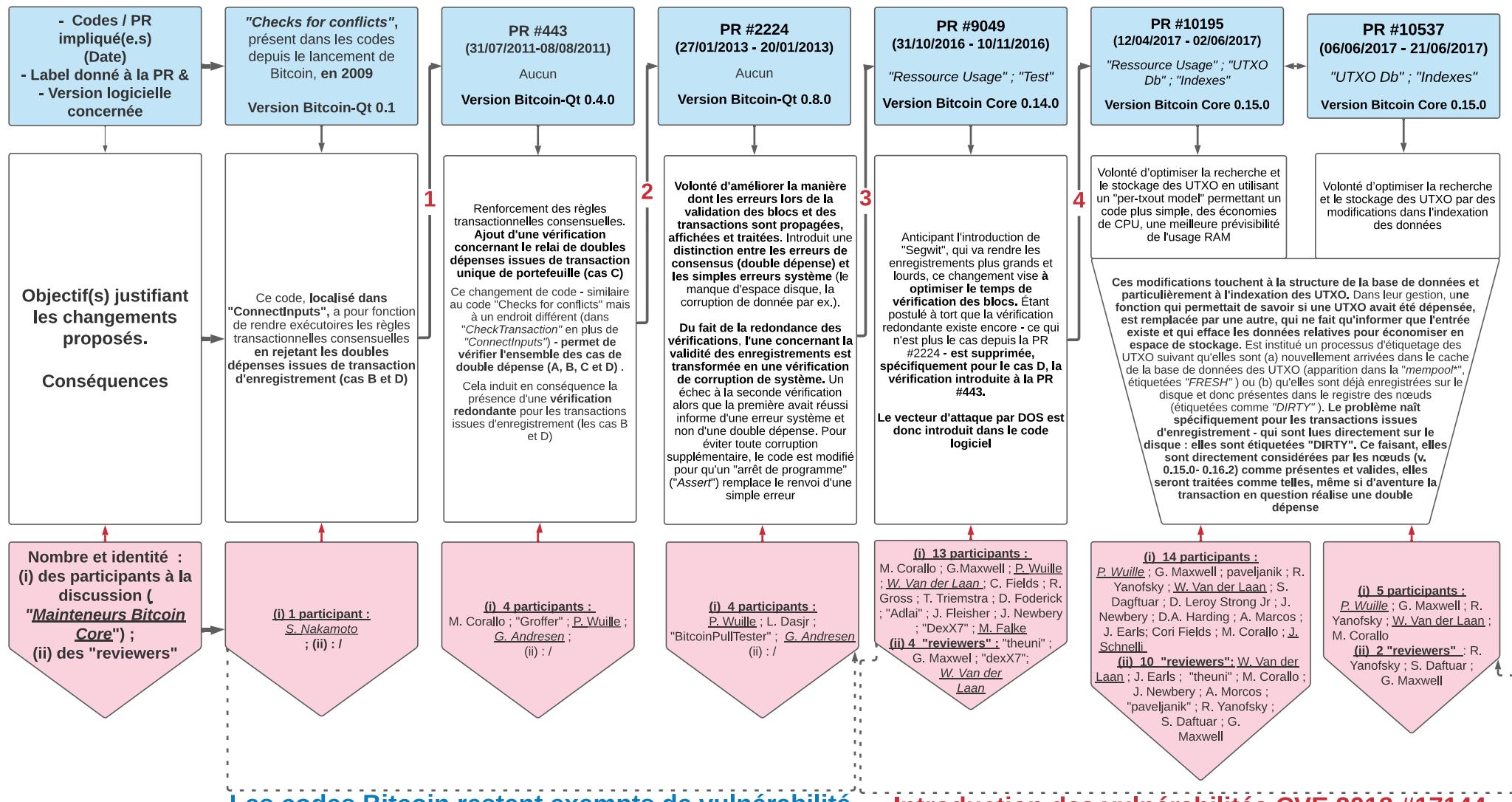
³²⁴ Voir <https://github.com/bitcoin/bitcoin/pull/443> [consultation au 12/09/2021].

³²⁵ Similaire à la fonction « *Check for conflicts* »/« *vSpent* », mais localisée ailleurs, dans « *CheckTransaction* » (Song, 2018).

³²⁶ Suivant deux processus, une fois *via* « *CheckTransaction* » et une autre *via* « *ConnectInputs* » (Song 2018).

³²⁷ Voir <https://github.com/bitcoin/bitcoin/pull/2224> et <https://github.com/bitcoin/bitcoin/pull/2224/files> [consultation au 12/09/2021].

Figure 9 : D'une sédimentation de modifications des codes Bitcoin de 2011 à 2017 créant la faille



En octobre 2016, M. Corallo propose la PR 9049³²⁸ qui vise à accélérer le temps de vérification pour des enregistrements voués à être plus lourds (en taille mémoire), après la mise à jour « SegWit » annoncée (cf. « Scaling Debate », Chap. II section II.3.3). Corallo postulant à tort que la vérification redondante précédente existe encore (ce qui n'est plus le cas depuis la PR 2224), il propose sa suppression, afin « *d'éviter une vérification coûteuse lors de la validation* initiale du bloc pré-relais que les entrées multiples au sein d'une même transaction* ne dépensent pas deux fois la même entrée, ce qui avait été ajouté en 2012 (PR #443)* » (Bitcoin Core 2018a). Dans la mesure où l'évaluation des PR erronées de Corallo est partagée entre les participants³²⁹ et que « *les résultats du benchmark indiquent [une économie d']environ 0,5-0,7 ms* » (M. Corallo³³⁰), l'optimisation est acceptée et fusionnée au répertoire logiciel principal. La première itération du bogue CVE 2018 dans les versions Bitcoin Core 0.14.0 est introduite ainsi. Désormais, sans qu'aucun acteur n'y prête attention, les nœuds* fonctionnant sur cette version sont devenus vulnérables (cf. Tableau 3 suivant pour une estimation) et toute « *tentative de dépenser deux fois la sortie d'une transaction* au sein d'une transaction* unique dans un bloc entraînera [...] un plantage* » (Bitcoin Core 2018). L'introduction de l'itération de « faux monnayage » par double dépense renvoie, elle, à l'articulation de deux PR distinctes : les PR n° 10195 et n° 10537, discutées entre avril et juin 2017³³¹. La PR n° 10195, émanant de P. Wuille, sera discutée par 14 participants, dont 10 sont formellement relecteurs³³². Elle vise à optimiser la recherche et le stockage des UTXO* via un code plus simple (substitution de la base de données et du cache à un modèle « per-txout ») permettant des économies de CPU et une meilleure prévisibilité de l'usage de la mémoire RAM (P. Wuille³³³). La PR n° 10537 émane

³²⁸ Voir <https://github.com/bitcoin/bitcoin/pull/9049> [consultation au 12/09/2021]. M. Corallo justifie cette PR comme suit : « *Bitcoin Core est très optimisé [...] quand votre nœud* reçoit un bloc, il fait autant de vérifications que nécessaire et ensuite il transmet le bloc. [C'est] une partie clef de la résistance contre [certaines] attaques [...] pour la rentabilité du minage et pour avoir [...] une distribution équitable de la rentabilité du minage. [...] dans le contexte de la validation* complète des blocs, il ne s'agit pas d'une optimisation majeure [...]. Mais entre le moment où Bitcoin Core reçoit un bloc et le relâche à ses pairs, il ne fait qu'une sorte de vérification initiale [...] de la preuve de travail. Il s'agit de s'assurer que la copie du bloc est en quelque sorte une bonne copie [...] non modifiée, donc il s'assure qu'il est comme le bloc canonique et qu'il a la preuve du travail [...]. C'est suffisant pour se rendre compte qu'il n'y a aucune raison de dire que j'ai besoin de valider complètement le bloc avant de le relayer parce qu'on sait avoir déjà vérifié [...]. C'est fondamentalement une vérification redondante et c'est quelque chose qui ralentit matériellement la propagation des blocs et donc il faut s'en débarrasser. [...] Cette bonne idée s'est avérée comporter plus de risques que nous l'avions prévu et les vérifications réelles, plus lointaines dans le code, se sont avérées ne pas protéger contre cela et n'ont tout simplement pas été prises en compte à l'époque.* » [Entretien n°15]

³²⁹ Pour les acteurs, les PR impliquées sont floues : « *les développeurs*, lorsqu'ils ont discuté du PR 9049, étaient prédisposés à penser qu'une double dépense simple-tx au niveau du bloc [...] était vérifiée ailleurs à partir du PR 443 sans tenir compte du PR 2224 [et ils n'ont] pas examiné aussi attentivement le PR 9049* » (Song 2018). Les échanges IRC « Bitcoin Core Dev » révèlent l'impact du temps long : « <Sipa> : Avons-nous même besoin de cette vérification ? <Bluematt> : Celui des entrées dupliquées ? Pas clair, probablement pas mais nous l'avons ajouté pour une raison. <BlueMatt> : Je ne me souviens pas de ce que c'était... <BlueMatt> : Je me souviens cependant que nous avions une raison. « <BlueMatt> : Oui, et je me rappelle avoir eu une raison [...] <BlueMatt> : Je veux dire que c'était il y a longtemps » (Song 2018).

³³⁰ Voir le fil de discussion Github suivant <https://github.com/bitcoin/bitcoin/pull/9049> [consultation au 12/09/2021].

³³¹ Voir <https://github.com/bitcoin/bitcoin/pull/10195> et <https://github.com/bitcoin/bitcoin/pull/10537> [consultation au 13/09/2021].

³³² Les discutants sont : P. Wuille, il est à l'origine de la proposition et de la fusion de cette PR dans le répertoire principal ; G. Maxwell ; paveljanik ; R. Yanofsky ; W. Van der Laan ; S. Dagftuar ; D. Leroy Strong Jr ; J. Newbery ; D.A. Harding ; A. Marcos ; J. Earls ; Cori Fields ; M. Corallo ; J. Schnelli. Les relecteurs formellement reconnus sont : W. Van der Laan ; J. Earls ; "theuni" ; M. Corallo ; J. Newbery ; A. Marcos ; "paveljanik" ; R. Yanofsky ; S. Daftuar ; G. Maxwell ; voir <https://github.com/bitcoin/bitcoin/pull/10537> [consultation au 14/09/2021].

³³³ Commentaire introductif du 12 avril 2017, <https://github.com/bitcoin/bitcoin/pull/10195> [consultation au 16/09/2021].

de M. Corallo. Elle sera discutée par 5 participants, dont 2 sont formellement relecteurs³³⁴. Il s'agit encore d'optimiser la recherche et le stockage des UTXO* (*via* l'indexation des UTXO* et la sémantique d'assertion « per-UTXO* ») et, par-là, le traitement des données par les nœuds*. Complémentaires, ces deux PR participent d'*« une refonte plus large visant à simplifier le suivi des sorties de transaction* non dépensées et à corriger une attaque par épuisement des ressources »* (Bitcoin Core 2018) : pour économiser de l'espace de stockage, une fonction renseignant si une UTXO* a été dépensée est remplacée par une se limitant à dire si l'entrée existe³³⁵. Ces deux PR rendaient « *le code autour du stockage UTXO** » - une « *partie clé du code de consensus* » - « *beaucoup plus simple* » [et était] aussi un peu plus efficace à [d'autres] égards » [M. Corallo, Entretien n°15]. Elles sont ainsi acceptées et fusionnées dans les codes Bitcoin Core par P. Wuille, sans controverse. Mais, ce qui est « *beaucoup plus simple, [ne] signifie pas que c'est plus facile à auditer et beaucoup plus net* » [M. Corallo, Entretien n°15]. À l'insu de tous, l'itération de la faille de « faux monnayage » est introduite dans Bitcoin au sein des versions 0.15.0 (publiée le 14 septembre 2017) à 0.16.2 (publiée le 29 juillet 2018)³³⁶. Les nœuds* concernés par les versions vulnérables traiteront toute transaction* issue d'enregistrements passés comme valides : directement lue sur le disque, où toute transaction* existante l'est par définition, un cas de double dépense sera valide, permettant « *à un mineur de gonfler l'offre de bitcoins [en] revendiqu[ant] la valeur dépensée deux fois* » (Bitcoin Core 2018).

Au temps long de cette phase d'insémination/gestation va répondre un déclenchement et une période de remise en ordre courte.

D'un déclenchement confidentiel par « divulgation responsable »

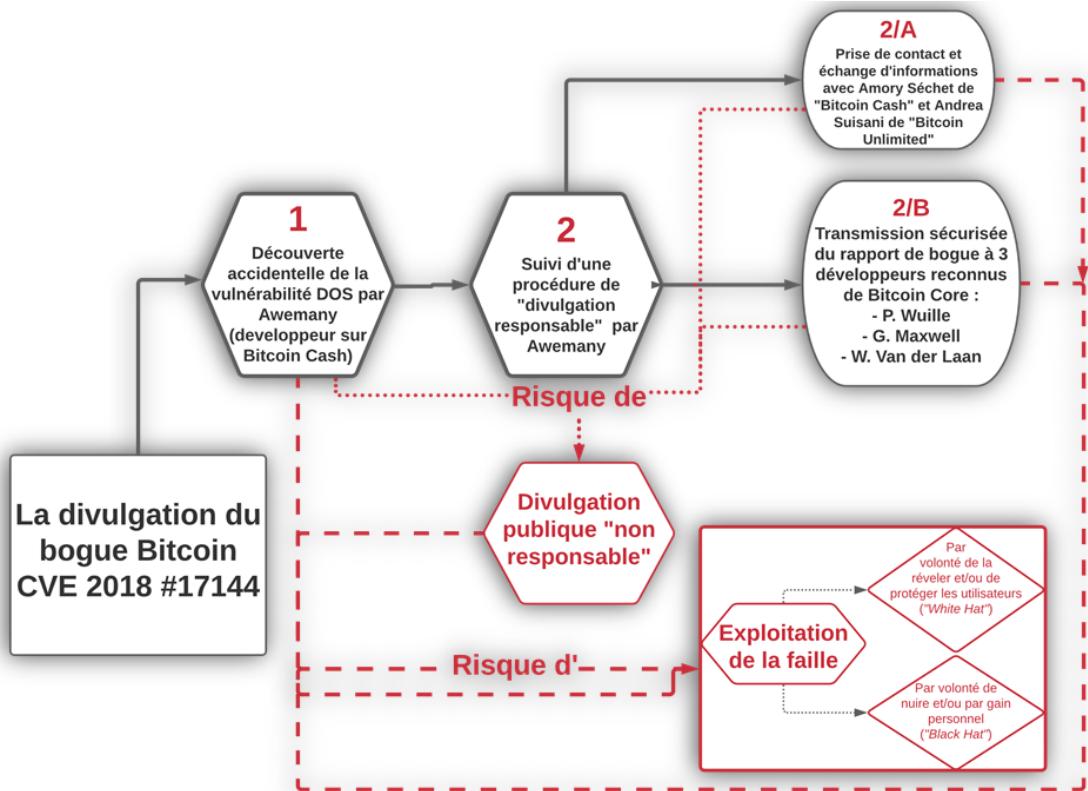
Le déclenchement renvoie au moment où des codes se voient reconnaître le statut de vulnérables par un ou plusieurs acteur(s). Ici, cette reconnaissance fut privée, secrète et silencieuse, comme le révèlent les conditions d'accès asymétrique aux informations concernant la faille (représentées dans la Figure 10 suivante). Ces conditions nous permettent de distinguer, d'un côté, un groupe d'initiés, numériquement réduit et bénéficiant d'un accès privilégié à des informations et, d'un autre, un ensemble large d'acteurs regroupant le commun des utilisateurs, qui dépend du premier groupe pour ce qui est de son accès à l'information et à la connaissance. J. Song [Entretien n°14] confirme cette distinction très naturellement quand nous en venons à expliciter les conditions par lesquelles il eut connaissance des évènements : « *j'en ai entendu parler de la même manière que n'importe qui d'autre, j'ai vu la divulgation faite par les développeurs* de Bitcoin Core* ». Partant de la découverte de la faille, intéressons-nous à ce groupe d'initiés par qui l'entrée en crise se fait.

³³⁴ Les discutants sont : P. Wuille, qui, en plus d'être à l'origine de la proposition, va être celui qui, disposant des droits d'administrateur* sur le répertoire, fusionnera cette PR dans le répertoire principal ; G. Maxwell ; R. Yanofsky ; W. Van der Laan ; M. Corallo. Les relecteurs formellement reconnus sont : R. Yanofsky ; S. Daftuar ; G. Maxwell ; voir <https://github.com/bitcoin/bitcoin/pull/10195> [consultation au 16/09/2021].

³³⁵ Par institution d'un processus d'étiquetage des UTXO les qualifiant de « *FRESH* », si elles sont nouvelles dans la mempool*), ou de « *DIRTY* », si elles sont déjà présentes dans le registre* des nœuds*, ce qui permet de supprimer les données de transaction des secondes, dont la seule preuve de l'existence passée suppose leur validité (Anonyme 2018).

³³⁶ Pour les versions précédentes, « *toute tentative de dépenser deux fois une sortie de transaction au sein d'une transaction unique dans un bloc où la sortie dépensée a été créée dans le même bloc, le même échec d'assertion se produira (comme cela existe dans le cas de test qui a été inclus dans le patch 0.16.3)* ». (Bitcoin Core 2018a)

Figure 10 : La divulgation du Bogue CVE 2018, ses étapes, ses risques et ses acteurs



Source : Rolland Maël

1– Le 17 septembre 2018, Awemany « dans [s]a petite camionnette au bord de la mer, [...] travaillait à l'implémentation des nouveaux opcodes CHECKDATASIG/-VERIFY [...] pour Bitcoin (Cash) [quand il a] remarqué que la validation* de bloc saut[ait] [l]e test » vérifiant les entrées dupliquées lors d'une transmission de bloc³³⁷ (Awemany 2018). C'est un vecteur d'attaque par DOS potentiellement grave³³⁸. Cette découverte implique des risques pour les CM concernées (en rouge). Le découvreur peut tout d'abord tenter d'exploiter la faille en secret : si le profit escompté est personnel, l'exploitation est considérée comme maligne, relevant de chapeau noir (ou « Black Hat ») ; dans le cas inverse, la qualification de chapeau blanc (ou « White Hat ») est retenue (comme dans la crise d'Ethereum, cf. section III.3.2). Ensuite, hors malice, la divulgation peut être qualifiée de « non responsable » si le découvreur diffuse largement les informations concernant la vulnérabilité, permettant que des acteurs mal intentionnés s'engagent dans son exploitation. Awemany ne choisit aucune des voies précédentes. En tant que « citoyen responsable dans cet écosystème » (*Ibid.*), il s'engage dans une « divulgation responsable » : il limite l'accès à cette information cruciale à un petit nombre d'acteurs reconnus, et réduit d'autant les risques que ferait courir sa diffusion au plus grand nombre. Au moment de sa découverte, il contacte d'abord ses collègues de l'équipe de

³³⁷ Vérification « CheckRegularTransaction » pour Bitcoin ABC, « CheckTransaction » pour « Bitcoin Core » (Awemany 2018).

³³⁸ Il décrit s'être dit : « "Oh putain, ça n'a pas l'air bon, je dois prévenir deadalnix et l'équipe de ce qui se cache dans ABC, ça n'a pas l'air bon du tout. \$@#% !!" Conscient du danger que cela pourrait peut-être être exploité plus avant vers un véritable bug d'inflation et de séparation de chaîne (mais je n'ai pas vérifié plus [...] car un bug de plantage de nœud* avec échec de assert était déjà suffisant » (Awemany 2018).

développement Bitcoin ABC. C'est une fois l'alarme donnée « chez lui » qu'il s'engage dans une procédure de « divulgation responsable » à l'adresse d'équipes de développement extérieures, travaillant sur des implémentations de CM potentiellement exposées (*Ibid.*) : l'équipe de développement des implémentations « *Bitcoin Unlimited* » (client Bitcoin et Bitcoin Cash) et celle de « *Bitcoin Core* » (client référent pour Bitcoin).

2 – En s'engageant dans un processus de divulgation responsable, Awemany souhaite « *jouer franc jeu* » (Awemany 2018), ce qui n'a rien d'aisé dans le champ des CM (Fields 2018 ; Awemany 2018 ; Böhme et al. 2020). Son rapport sur la faille DOS rédigé, encore devait-il être en mesure de l'adresser aux bons acteurs (les « responsables » dans la communauté considérée) et ce, de manière confidentielle et sécurisée. Cette possibilité repose sur l'existence d'une liste de personnes contacts en charge de la sécurité, c'est-à-dire un groupe d'acteurs formellement reconnus comme étant en charge du développement et de la maintenance des implémentations logicielles. En plus d'identifier les contacts, il faut aussi utiliser les voies de communication sécurisées ouvertes (assurant la confidentialité, l'authenticité des informations transmises et des intervenants). Conventionnellement, c'est une page de contact sur le site web de l'implémentation logicielle considérée qui explicite les processus de divulgation de vulnérabilité établis. Dans tous les cas, il est attendu « *que les développeurs* fournissent des clés publiques avec leur contact de sécurité*³³⁹ et *qu'ils disposent de processus internes pour traiter les messages entrants* » : ce qui, dans le champ des CM, est loin d'être le cas, même pour des CM d'envergure (Fields 2018, repris par Böhme et al. 2020, p. 68). Fields (2018), lors d'une divulgation d'un bogue précédemment découvert sur l'implémentation Bitcoin ABC, disait s'être « *heurté à un mur* », car « *aucune clé n'était répertoriée [...] sur les serveurs de clés PGP publics où on les trouve habituellement, [ni] dans leur dépôt de code* ». Même problème pour Awemany, la liste de contacts trouvée est obsolète : il rejoint « *Cory Fields de Core* » sur la difficulté « *de trouver les adresses et les informations de divulgation nécessaires* » (*Ibid.*), et précise que le « *manque de clés PGP facilement accessibles* » pour Bitcoin ABC est aussi vrai pour Bitcoin Core, n'ayant « *pas trouvé à temps une clé non rétractée*³⁴⁰ de Pieter Wuille » (Awemany 2018). Du fait de sa position de développeur* sur Bitcoin ABC, Awemany n'a rencontré aucune difficulté à contacter les membres des équipes de « *Bitcoin Cash* »³⁴¹ et de « *Bitcoin Unlimited* »³⁴² (2/A, cf. figure précédente). Le contact avec les membres de l'équipe « *Bitcoin Core* » a été plus compliqué (2/B, cf. figure précédente). Le site Internet dispense des informations précises sur les procédures relatives à la divulgation de vulnérabilité. Deux processus sont distingués : si la faille ne touche pas à la sécurité du logiciel, un simple processus de suivi des problèmes publics (ou "Public Issue Tracking") est suffisant ; dans le cas inverse, une divulgation responsable s'impose et il est demandé de se reporter aux mails et clef de chiffrement donnés par la liste de contacts³⁴³, si tant est qu'elle soit à jour. Le rapport de divulgation sera finalement transmis le même jour, via « *message PGP crypté* » à l'adresse d'un « *ensemble de personnes de confiance* » (Awemany 2018 ; confirmé par Bitcoin Core 2018) : P. Wuille, G. Maxwell & W. Van der Laan, trois développeurs*

³³⁹ L'accès aux adresses mails et aux clefs publiques de chiffrement PGP garantit l'identité des acteurs, l'intégrité des informations échangées et leur confidentialité.

³⁴⁰ Lors de la création d'une clef PGP, une date d'expiration est définie et un certificat de révocation est émis. La date d'expiration doit être prolongée par leurs détenteurs et, en cas de perte de la clef privée, il est possible de la révoquer.

³⁴¹ En l'espèce, Amaury Séchet travaillant sur l'implémentation « *Bitcoin ABC* » (voir Awemany 2018).

³⁴² En l'espèce, Andrea Suisani travaillant sur l'implémentation « *Bitcoin Unlimited* » (voir Awemany 2018).

³⁴³ Voir <https://bitcoin.org/en/bitcoin-core/contribute/issues>. et <https://bitcoincore.org/en/contact/> [consultation au 17/09/2021].

Bitcoin Core reconnus³⁴⁴. À sa réception, Bitcoin et les membres informés de l'équipe Bitcoin Core entrent en crise. L'amorce d'une remise en ordre nécessite d'évaluer la vulnérabilité afin d'élaborer, de discuter et de tester les remédiations potentielles, avant qu'elles ne soient acceptées par la communauté.

Une remise en ordre rapide

Après réception du rapport d'Awemany, les trois « Core Devs » doivent d'abord réaliser un diagnostic interne de la situation, avant de proposer, discuter, produire et tester des correctifs.

La phase d'évaluation : définition des problèmes, des solutions et d'une stratégie de résolution

Le diagnostic de la faille Bitcoin CVE 2018 prend moins d'un jour à une poignée d'acteurs qui vont l'évaluer, puis développer un correctif logiciel et le faire évaluer en retour par des pairs, en vue de sa validation*/fusion dans les codes source d'une nouvelle version logicielle. D'après le rapport de divulgation complet de Bitcoin Core (2018), cette phase d'évaluation renvoie à 8 étapes clefs.

(1) G. Maxwell, l'un des contacts de sécurité et destinataire du rapport le fait suivre à réception à quatre autres « Core Devs » pour évaluation approfondie : C. Fields, M. Corallo, S. Daftuar et A. Morcos. M. Corallo, qui travaille avec Daftuar et Morcos à « Chaincode Lab »³⁴⁵, rapporte l'avoir trouvé sur son bureau « *quand [il est] arrivé le matin de son signalement...* » et c'est ensemble qu'ils entreprennent son analyse [M. Corallo, Entretien n°15]. (2) Cette évaluation interne fait apparaître un bogue plus critique que rapporté, scellant du même coup la stratégie d'une libération graduelle des informations. Si « *à l'origine, il a été signalé comme un crash. [...]. [Après un] temps à l'examiner, à lire le code [...], nous avons découvert la véritable vulnérabilité d'inflation* [, dès lors] *il s'agissait de savoir comment minimiser le risque pour les utilisateurs de Bitcoin [et] la réponse immédiate est... d'écrire un patch [...]. Heureusement cela nous a été rapporté comme un crash et l'exploit évident était le crash et non la vulnérabilité d'inflation. Donc la décision était... [...], de publier le crash, de parler aux gens du crash et [...] de diffuser le patch [...] qui résout une vulnérabilité réellement critique sans nécessairement mentionner l'autre vulnérabilité, plus critique encore* » [M. Corallo, Entretien n°15]. Afin de minimiser les risques pour les utilisateurs, ces Core développeurs* décident d'occulter le bogue de faux monnayage, en insistant uniquement sur le vecteur de DOS. Toute faille confronte les personnes en charge d'y remédier à un dilemme : publier un correctif, c'est avouer publiquement l'existence d'une vulnérabilité, ce que le processus de divulgation responsable vise à cacher. D'où le « *jeu d'annoncer la vulnérabilité la plus évidente* » (la faille

³⁴⁴ Tous deux « Core Devs » de longue date, P. Wuille et W. Van der Laan sont des « Core Maintainers » disposant de droits d'administration sur le répertoire Bitcoin Core (Lopp 2018) et comptent parmi les plus actifs (voir Gaurav 2019) ; Wuille, avec G. Maxwell, fait partie des co-fondateurs de l'entreprise « Blockstream » (comme M. Corallo). Il a renoncé à ses priviléges d'administration en 2015, mais reste un développeur reconnu. Voir : <https://github.com/laanwj> , <https://github.com/sipa> (voir bit2me Academy 2021) , https://www.reddit.com/r/Bitcoin/comments/3x7mrr/gmaxwell_unllc_no_longer_a_bitcoin_committer_on/cy29vkx/ et <https://github.com/gmaxwell> [consultation au 17/09/2021].

³⁴⁵ « Chaincode Lab » est une entreprise de recherche et développement dans l'écosystème Bitcoin, créée en 2014, dont M. Corallo était à l'époque encore salarié. Cette compagnie fut fondée par A. Morcos et S. Daftuars, deux « Core Devs » actifs et reconnus qui sont aussi co-fondateurs d'une société de trading « Hudson River Trading ». Ils se décrivent comme « *passionnés par la progression du développement du réseau Bitcoin et par la fourniture de ressources aux innovateurs indépendants de l'écosystème Bitcoin* » ; ils sont « *financés par des fonds privés* » et existent « *pour soutenir et développer Bitcoin* ». En 2020, cette entreprise est « *le leader incontesté en termes de financement des développeurs* de Bitcoin Core* » (BitMEX Research 2020). Voir : <https://github.com/morcos> , <https://github.com/sdaftuar>, et <https://chaincode.com/> [consultation au 17/09/2021].

de déni de service), ce qui est ensuite utilisé « *comme un moyen de pousser les gens à mettre à jour aussi vite que possible [...] ce qui résout tous les problèmes* [M. Corallo, Entretien n°15]. Cette stratégie de divulgation fait coup double : en plus d'éclipser la faille touchant au faux monnayage, ne parler que de risques de DOS permet d'inciter les opérateurs de nœuds* (mineurs et/ou complets) à mettre à jour rapidement leurs logiciels clients : « *obtenir immédiatement du hashrate de minage avec le patch* » permet de sécuriser au plus vite le réseau*, le protocole et ses règles canoniques contre les effets délétères de cette faille. D'où le fait que, à l'étape suivante (3), M. Corallo tente de transmettre en privé le correctif à « Slush pool », une pool de minage amie, « *plus facile et fiable à contacter que beaucoup de pools chinoises* », sans pour autant le diffuser publiquement. Cette volonté renvoie à deux objectifs. D'abord, une évaluation par les pairs du correctif dans le respect des principes contenus dans les slogans des *coiners** (« *don't trust verify* » et « *Do Your Own Research* ») : pour ne pas être « *dans une position où Bitcoin Core dit de sauter et tout le monde saute* », des développeurs* extérieurs, reconnus et de confiance, doivent non pas « *juste [l']exécuter aveuglément* »³⁴⁶ [M. Corallo, Entretien n° 15], mais l'analyser et le tester indépendamment afin de vérifier qu'il corrige l'attaque DOS annoncée sans introduire de nouveaux problèmes, la sécurité de leur activité en dépend. Ensuite, cela sécurise une partie du réseau* avant même que soit révélé publiquement le correctif, car « Slush Pool » représentait près de 10% de la capacité de calcul du réseau*³⁴⁷. Cette stratégie garantit que le réseau* Bitcoin repose sur une puissance de calcul « *patchée* » avant la libération publique des informations, réduisant le risque d'exploitation par des individus mal intentionnés, qui auraient compris le périmètre réel des vulnérabilités corrigées par le correctif. Cependant, aucune communication n'a pu être établie avec son CEO. (4) Étape où G. Maxwell établit une preuve de la découverte de la vulnérabilité de « faux monnayage », sous la forme d'un horodatage* du *hash** du test de la vulnérabilité réalisé (Bitcoin Core, 2018)³⁴⁸. La production de cette trace vérifiable et non falsifiable permettra de confirmer les annonces futures de l'équipe Bitcoin, renseignant une volonté des acteurs de documenter la gestion des événements afin d'offrir à la communauté des éléments de transparence *a posteriori*. (5) À cette étape, la propagation des informations au-delà du premier cercle des initiés commence. J. Newbery et J. O'Beirne (Bitcoin Core 2018), qui travaillent chez « Chaincode labs » avec Corallo, Daftuar, Morocos, sont informés de la faille DOS et chargés d'alerter en privé différentes entreprises du secteur, en les prévenant qu'un correctif sera bientôt disponible. (6) Cette étape voit Corallo établir le contact avec J. Capek et P. Moravec, respectivement CEO et CTO de Slush Pool. Le correctif leur est transmis et, par téléphone, eux aussi discutent uniquement du bogue DOS : « *nous leur avons envoyé le patch et ils nous ont renvoyé des questions. [...] Ils ont regardé le patch, ils l'ont analysé et nous ont posé des questions à son sujet. Nous avons répondu et ils ont pu l'appliquer assez rapidement* » [M. Corallo, entretien n° 15]. (7) Slush Pool met à jour ses logiciels clients dès la fin de journée du 17 septembre, sécurisant ainsi 10% de la puissance de calcul du réseau* contre la vulnérabilité DOS et celle de « faux monnayage ». Le 18 septembre, l'équipe Core produit et

³⁴⁶ Ces attendus étaient explicites dans le message envoyé à Slush Pool. Corralo déclare avoir essayé « *d'être un peu précautionneux et de dire : voilà le patch, voilà ce qu'il fait, s'il vous plaît vérifiez, ne prenez pas juste le patch et exécutez-le aveuglément... non s'il vous plaît vérifiez qu'il fait quelque chose qui ressemble à ce que nous prétendons [...] d'autant plus que nous leur avons envoyé un patch qui n'était pas public et qui n'était pas audible.* » [M. Corallo, Entretien n° 15]

³⁴⁷ Au 17 septembre 2018, Slush Pool représentait 9,3% de la puissance de calcul du réseau Bitcoin, voir <https://web.archive.org/web/20180916150610/https://www.blockchain.com/pools> [consultation au 17/09/2021].

³⁴⁸ Ce *hash** est le suivant a47344b7dceddff6c6cc1c7e97f1588d99e6dba706011b6ccc2e615b88fe4350 (Bitcoin Core 2018).

publie les binaires logiciels des versions correctives et des annonces publiques annoncent la mise à jour comme « urgente » (8).

La phase d'évaluation touche à sa fin. La résolution amorcée commande encore de produire, publier et publiciser les logiciels corrigés et d'informer l'ensemble de la communauté.

La phase de résolution : « mensonge blanc » contre « chapeau noir »

La phase précédente est une amorce nécessaire mais non suffisante à toute remise en ordre définitive. Il importe maintenant qu'une majorité, si ce n'est la totalité des opérateurs de nœuds* vulnérables, consente à les mettre à jour rapidement. C'est une phase nécessaire, car elle permet de fixer et discuter entre un petit nombre d'acteurs compétents des problèmes techniques existants et des solutions potentielles. Ce bogue « *très simple* » (equobleu 2018) ne prend que quelques heures à M. Corallo pour être corrigé. Les correctifs, publiés sous forme de Pool Request (les PR#14247 et PR #14249)³⁴⁹, n'impliquent qu'une modification de « *4 lettres (vrai au lieu de faux)* » dans les codes sources et l'ajout d'un « *test automatisé [...] pour tester le scénario du bloc avec des pièces (en "entrée") dépensées en double* » (*Ibid.*)³⁵⁰. Reste que cela est insuffisant. La confidentialité offerte par la dimension *off chain** a permis de recourir, comme par le passé³⁵¹, à des silences stratégiques et « *mensonges blancs* », visant à produire « *une tromperie délibérée des utilisateurs* » pour mieux les protéger contre les attaques potentielles, qu'une publicité large n'aurait pas manquée d'induire (Böhme et al. 2020, p. 68). Mais cette mise au secret n'a qu'un temps. Les informations dispensées ne concernent encore qu'un petit groupe de participants là où, pour une CM, toute résolution de crise passe par la sécurisation de l'ensemble du réseau*, donc par une publicisation large et risquée des correctifs : les mensonges blancs précédents se doivent d'être éprouvés largement, une dernière fois.

Nous rencontrons là une problématique épingleuse de la gouvernance de crise de Bitcoin et des CM, ces « *systèmes distribués [...] ont été conçus pour être difficiles à modifier afin de fournir de solides garanties sur leur comportement futur.* » (Böhme et al 2020, p. 64). Par design, toute modification de code implique nécessairement un consentement - anonyme, organisé de manière lâche et informelle - de la multitude des participants la concernant (*Ibid.*). Toute modification de code est un « *coordination challenge* » puisqu' « *aucun développeur* ou mainteneur n'a naturellement le rôle de coordonner la correction des bogues, et encore moins l'autorité de déployer des mises à jour contre la volonté des autres participants* » (*Ibid.*). Mais ce qui précède l'a révélé, Bitcoin et son implémentation « *Bitcoin Core* » disposent d'un groupe de mainteneurs Core plus que « *vaguement définis* », assumant formellement la gestion

³⁴⁹Les PR #14247 et #14249 voient deux modifications (« commits » dans le jargon des développeurs* informatiques) être fusionnées dans la branche maître Bitcoin Core (« bitcoin :master »); voir <https://github.com/bitcoin/bitcoin/pull/14249> et <https://github.com/bitcoin/bitcoin/pull/14247> [consultation au 07/10/2021].

³⁵⁰ La ligne de code 3125, “if (!CheckTransaction(*tx, state, false))” devient “if (!CheckTransaction(*tx, state, true))” et le test (test/functional/p2p_invalid_block.py) est ajouté à la ligne 81. Voir <https://github.com/bitcoin/bitcoin/pull/14247/files#> et/ou <https://github.com/bitcoin/bitcoin/pull/14249/files> [consultation au 07/10/2021].

³⁵¹ Böhme et al. (2020) rappellent que, en 2014, une incohérence entre différentes versions de la bibliothèque OpenS-SL présente au sein de version logicielle Bitcoin avait déjà donné lieu à ce type de « *mensonge blanc* » : « *la correction d'OpenSSL n'était pas une option, d'où la nécessité d'appliquer [d]es changements [...] de manière subtile et progressive afin d'éviter d'attirer l'attention sur le morceau de code concerné. Les utilisateurs ont procédé à une mise à niveau organique sur une période de 10 mois. Le bogue a été rendu public lorsque plus de 95% des mineurs l'ont corrigé* » (p. 68).

coordonnée de la résolution des bogues (*Ibid.*). Reste que ce groupe n'est pas capable d'imposer aux autres parties ces modifications, ses membres ne disposant que de leur connaissance et persuasion. Puisqu'ils travaillent sur un logiciel à code source ouvert, tournant de manière distribuée, les mainteneurs Bitcoin Core ne disposent d'aucun moyen pour imposer une nouvelle version logicielle aux opérateurs de nœuds* mineurs ou complets. Pour faciliter le consentement éclairé *ex ante* nécessaire à ce que tous téléchargent et se mettent à jour *ex post*, il a été institué une procédure séquentielle. Premièrement, les modifications proposées doivent être accessibles publiquement *via* le répertoire Github de « Bitcoin Core » (le « *repo* »), publiées sous forme de PR ou de « *BIP* ». Cela permet qu'elles soient évaluées et discutées. Enfin, en cas de soutien majoritaire ou plus exactement d'opposition minoritaire³⁵², ces PR sont ensuite fusionnées dans les codes sources d'une nouvelle version logicielle. De ceux-ci, il faut encore produire des binaires logiciels accessibles au téléchargement par l'ensemble de la communauté.

Aux coordinations challenges « intracommunautaires » s'ajoute, pour la CM et l'équipe de mainteneurs qui publient les correctifs, un challenge « extra-communautaire » du fait de la nature open source des codes vulnérables. Cela accentue l'ambivalence du moment crucial qu'est la publication d'un correctif dans la gestion de crise. La faille de « faux monnayage », pour l'heure tenue sous silence, pourrait être découverte. La coordination avec d'autres équipes de CM partageant les codes vulnérables de Bitcoin Core ajoute à la complexité, d'autant qu'il existe des liens d'amitié ou d'inimitié entre ces équipes. Dans l'idéal, les « *correctifs doivent être déployés aussi simultanément que possible dans tous les projets concernés, car l'application de correctifs et la publication d'informations sur la vulnérabilité laisseraient d'autres personnes exposées si aucune précaution n'était prise.* » (Böhme et al 2020, p. 70) Dans la réalité des crises, l'idéal fait place à des réponses plus contraintes. Dans ce cas, les mainteneurs Core ont d'abord, avant toute publicisation des correctifs, envoyé un mail à l'équipe de Bitcoin ABC, pour les avertir de la publication prochaine du correctif au public (Bitcoin Core 2018). De même, fut envoyée une réponse de remerciement à Awemany, auteur du rapport anonyme. Ces précautions prises, critiquables car insuffisantes pour certains³⁵³, les correctifs sont publiés dès la fin de journée du 17 septembre (*Ibid.*). Moins d'une heure après l'envoi des mails d'alerte aux équipes de projets différents³⁵⁴, la démonstration du test de l'attaque par DoS est publiée sur le « *repo* » public « Bitcoin Core » (la PR #14247). Dans la foulée, une campagne de communication visibilisant le bogue et son correctif est lancée à l'adresse de différentes listes de diffusion (*Ibid.*). Dans la soirée, une nouvelle version logicielle

³⁵² Comme nous le verrons, le consensus ne renvoie pas tant à un fait majoritaire selon une définition de la majorité, ni même à une unanimous, puisque s'abstenir correspond à ne pas s'opposer, qu'à l'absence d'opposition franche. La définition d'un consensus communautaire large et les outils de sa mesure sont problématiques, d'où l'existence de controverses et l'expérimentation de procédures d'expression des désaccords variés, toujours évolutives et mouvantes (cf. section III.3).

³⁵³ Les acteurs de la communauté Bitcoin Cash sont critiques, considérant avoir été mis au pied du mur par une divulgation irresponsable de l'équipe Bitcoin Core (Awemany 2018, A. Sechet voir <https://github.com/bitcoin/bitcoin/pull/14247#issuecomment-422603346> ou encore « ftrader » voir <https://github.com/bitcoin/bitcoin/pull/14247#issuecomment-422499799>; [consultation au 12/10/2021]. Cette controverse est nourrie de ressentiments remontant au schisme communautaire consécutif au « Scaling Debate » (cf. Chap. II). D'autres projets vulnérables, non informés, ne sont pas corrigés et l'un d'eux (« PigeonCoin ») subit une double dépense exploitant la faille pour près de 235 millions d'UCN, soit 25% de l'offre en circulation (Esteves 2018 ; Hertig 2018).

³⁵⁴ Le rapport de divulgation complète (Bitcoin Core 2018) établit que l'équipe Bitcoin Cash a publié son propre correctif une minute seulement après la publication du PR 14247 sur Bitcoin Core.

Bitcoin Core est « taggée » (version 0.17.0rc4³⁵⁵, *Ibid.*). La production des nouvelles versions logicielles téléchargeables doit attendre.

Au sein de Bitcoin Core, la création et la publication de nouveaux codes binaires logiciels suit une procédure collective de sécurité innovante, nommée « *Gitian Building* » (Wirdum 2018), nécessitant que plusieurs membres reconnus de la communauté produisent, chacun de son côté et de manière déterministe, des binaires similaires : « *les correctifs pour les branches master et 0.16 [...] soumis à l'examen public hier* » et « *la version 0.16.3 [...] étiquetée comme contenant le correctif [...]* », encore faut-il « *qu'un nombre suffisant de contributeurs connus [aient] reproduit la construction déterministe* » (Bitcoin Optech 2018). À ces conditions sont rendues disponibles au téléchargement les nouvelles versions logicielles, d'où l'importance des annonces réalisées visant une mobilisation communautaire large. Ainsi, la version 0.16.3, « taguée » tôt dans la matinée du 18 septembre, attendra le lendemain soir pour voir les premières versions être produites, publiées et ouvertes au téléchargement. Suite à cette publication, la publicisation s'intensifie. Au-delà des cercles techniciens premiers (exemple de la lettre d'information d'*« Optech »*³⁵⁶), des canaux de diffusion s'adressant à un public plus large sont mobilisés afin d'atteindre l'ensemble de la communauté : faille et correctif sont annoncés sur Reddit³⁵⁷ et BitcoinTalk³⁵⁸ ; le 19, une nouvelle campagne vise différentes listes de diffusion. Cette mobilisation de canaux d'information hétéroclites doit permettre la mobilisation large et rapide nécessaire à une mise à jour expresse, ordonnée et massive des clients logiciel, nombreux à l'époque des faits à être vulnérables. Les données montrent que ces campagnes d'information ont porté leurs fruits (voir le Tableau 3 ci-après).

³⁵⁵ Ces « tagues » ou « balises » sont des références permettant de marquer/nommer des points d'étape de l'historique de développement du projet et ses versions (v1.0, v1.0.1, v2.0 etc.). Sur ces procédures de développement logiciel, voir pour GIT (<https://git-scm.com/book/en/v2/Git-Basics-Tagging>) ou, spécifiquement pour Github (<https://docs.github.com/en/desktop/contributing-and-collaborating-using-github-desktop/managing-commits/managing-tags>). L'ensemble des différentes versions « taguées » Bitcoin Core historiquement publiées est consultable ici : <https://github.com/bitcoin/bitcoin/tags> [consultation au 08/10/2021].

³⁵⁶ Cette lettre d'information est adressée à des acteurs techniciens. L'édition du 18 septembre revient sur la vulnérabilité DOS et la publication des versions correctives Bitcoin Core 0.16.3 et 0.17rc4. Voir Bitcoin Optech (2018).

³⁵⁷ Voir <https://web.archive.org/web/20180918221912/https://www.reddit.com/r/Bitcoin/> [consultation au 08/10/2021].

³⁵⁸ Voir <https://bitcointalk.org/index.php?topic=5032424.0> [consultation au 08/10/2021].

Tableau 3 : Nombre et parts relatives des nœuds vulnérables³⁵⁹

Date	Nombre total de nœuds* Bitcoin	Somme & parts des versions vulnérables		
		Ensemble	Version 0.14.x	Version 0.15.x-0.16.x
18/09/2018	9590	82.56%	4,3%	78,3%
23/09/2018	9831	55.38%	0 %	55,38 %
23/10/2018	9847	38.6%	0 %	38.6%
01/01/2019	10162	23.43%	0 %	23.43%
28/06/2019	10318	11.24%	0 %	11.24%
07/01/2020	11204	6.16%	0 %	6.16%
23/09/2020	10000	4.89%	0 %	4.89%
25/06/2021	9909	4,28 %	0 %	4,28 %

Source : Rolland Maël

En juin 2021 encore, on trouve de rares nœuds* Bitcoin (moins de 5%) non encore mis à jour, restant exposés à ces vulnérabilités. Mais, à l'époque, la sécurisation du réseau* va s'opérer relativement rapidement : au 18 septembre, ce sont près de 82% des nœuds* qui étaient vulnérables (près de 4% pour la faille DOS et près de 78% pour celle de « faux monnayage » !!!!). Cinq jours après les premières annonces publiques, on ne trouve déjà plus aucun nœud* tournant sur les versions 0.14.x ; ceux fonctionnant sur les versions 0.15.x-0.16.x vulnérables, encore majoritaires, voient leur part baisser de près de 23%. Cette réactivité importe pour la sécurité de Bitcoin, car, ce même jour du 20 septembre, le mensonge blanc s'évante enfin : sur un forum public, un post fait état de la faille de faux monnayage et même s' « *il [a] été rapidement rétracté, l'affirmation a continué à circuler* » (Bitcoin Core 2018). Mais cette première libération publique n'a plus de quoi inquiéter l'équipe Bitcoin Core : « *plus de la moitié du hash*rate Bitcoin a été mis à niveau vers des nœuds* corrigés* » et si « *aucune tentative d'exploitation de cette vulnérabilité* » n'avait été décelée jusqu'alors, les possibilités de réussir une telle attaque s'amenuisent au fur et à mesure que le réseau* voit la part des

³⁵⁹ Ces estimations sont imparfaites. Tout d'abord, car notre première source, le site <https://coin.dance/nodes#nodeVersions> [consultation au 25/06/2021] ne décompte que le nombre de nœuds* Bitcoin publiquement accessibles. L'estimation est basse par construction, excluant les nœuds* non publics (passant par TOR par exemple, voir Luke Dashjr, luke.dashjr.org/programs/bitcoin/files/charts/). A. Le Calvez [Entretien n°20] précise que les données relatives aux implémentations et aux versions sont déclaratives et qu'il est impossible d'en prouver la véracité : « l'affichage du numéro de version c'est quelque chose d'optionnel, enfin d'optionnel, c'est dur à vérifier finalement. Puisque je peux faire croire que je suis un 0.14 alors qu'en fait je suis un programme qui n'est pas du tout un nœud* » (Entretien n°20). Puisque les données plus anciennes nous intéressent n'étaient pas accessibles sur « Coindance », nous avons mobilisé en complément la « Wayback Machine » d'« Internet Archive ». Cet outil dépendant des instantanés réalisés, nous n'avons pas pu choisir les dates. Nos estimations coïncident avec celle donnée par Bitcoin Core (2018).

nœuds* corrigés augmenter. (*Ibid.*). Au 20 octobre 2018, soit un mois après, la part des nœuds* vulnérables au « faux monnayage » tombait à 38 %, pour chuter, entre juin 2019 et janvier 2020, à moins de 10% du réseau*. Ce 20 septembre, alors que le secret bien gardé a commencé à s'éventer³⁶⁰ et puisqu'une part importante du réseau* a déjà été patché, l'équipe Bitcoin Core va mettre un point final à la crise : est publié le rapport de divulgation complète. Avec lui, est reconnue pour la première fois publiquement l'existence d'une faille impliquant un « faux monnayage » par double dépense (Bitcoin Core 2018). Le 21 septembre, Awemany sort de son silence et de l'anonymat, par la publication d'un billet de blog retraçant son implication dans les évènements (Awemany 2018). Ce texte prendra part, avec d'autres, à la controverse entourant la gestion de cette crise par l'équipe Bitcoin Core, qui, nous le verrons, est nourrie de ressentiments passés. Néanmoins, la crise traversée par Bitcoin et sa communauté est close : les vulnérabilités sont corrigées et révélées publiquement à tous, et le réseau* est déjà prémuni contre elles.

III.1.2 Restituer cette crise dans l'histoire de celles traversées par Bitcoin

Mettre en perspective les événements entourant la faille Bitcoin CVE 2018 nous forçait à ne pas s'arrêter à eux. Le questionnement sur la nature de cette crise pointait vers d'autres crises appelant à être démêlées : « ce n'est pas la première vulnérabilité à l'inflation [...] peu importe 0.1 ; 0.2, je ne me souviens pas des bogues de l'époque » [M. Corallo, Entretien n°15]. Impossible de ne pas voir ce que le Chapitre I a pris soin d'introduire : des crises nombreuses et diversifiées ont concouru au développement infrastructurel de Bitcoin, qu'elles aient été directement protocolaires (comme avec Bitcoin CVE 2018) ou plus largement infrastructurelles, touchant à des composants socio-techniques clefs à leur fonctionnement et usage (cf. bourse, portefeuilles* ; cf. Chronologie 2 Chap. I). D'où notre affirmation : non, la confiance et ses trois dimensions (éthique, hiérarchique et méthodique ; cf. Chap. II) ne se cristallisent pas tout entières dans le code ou seulement dans son *algorithme cryptographique*. Toutes les lignes de codes Bitcoin, comme l'ensemble des pathologies qui peuvent les toucher, n'ont pas la même importance pour son fonctionnement. Cela renvoie à l'existence de ce qui est pourtant nié explicitement (Dupré, Ponsot et Servet 2015) : une structuration sociale où se tiennent des débats politiques *hors chaîne**, au sein desquels se jouent aussi, et de manière complémentaire, les trois types de confiance.

En outre, de nombreuses informations concernant ces différentes crises étaient accessibles en ligne. Certaines émanent très directement d'un groupe d'acteurs pour qui ces préoccupations sécuritaires sont centrales (et dont Corallo fait partie). Même si nombreux sont les *coiners** à se désintéresser des crises que leurs CM pourraient rencontrer, il serait excessif, partial et faux de laisser penser que l'ensemble des « *bitcoincers** » partage une même « *foi dans le bitcoin* » et aurait une « *confiance aveugle exprimée [...] dans le code et l'algorithme* », alors que ceux-ci sont le produit d'acteurs éminemment conscients des risques et qui savent que toute technologie, en particulier celle qu'ils développent, est loin d'être « *infaillible* » (Ponsot 2021, p. 2). Dès l'origine, les CM sont conçues pour fonctionner dans un *environnement adverse* (Nakamoto 2008). Cela est même un critère définitionnel propre (Rauchs et al. 2018, cf. Chap. II). La sécurité de Bitcoin est suspendue à des conditions jamais données. Au-delà des seules « attaques 51% » sur lesquelles insiste le WP* de Nakamoto (2008), une variété de

³⁶⁰ En plus de la publication d'un premier message explicitant le bogue de consensus, le 20 septembre voit un autre développeur extérieur - David Jaenson, qui travaille sur le projet Qtum - découvrir indépendamment cette vulnérabilité (Bitcoin Core 2018, Hacker News Forum 2018). Il la rapporte à l'équipe Bitcoin Core le même jour, via la liste des e-mails de contact sécurité (Bitcoin Core 2018) et publiera le correctif sur le github du projet Qtum (Bitcoin Core 2018).

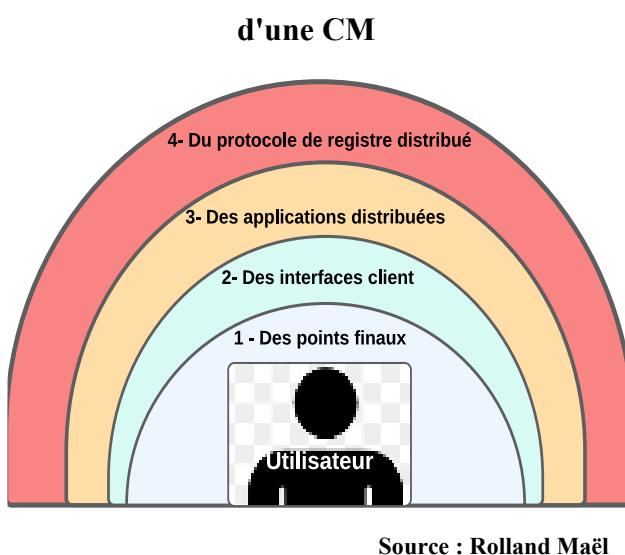
dysfonctionnements, voire d'attaques, existent, pouvant compromettre ses propriétés désirées (décentralisation, résistance à la censure*, pseudonymat, etc.).

De la diversité des crises aux crises protocolaires des CM

Bitcoin, comme infrastructure monétaire, repose primordialement sur l'articulation complexe de dispositifs techniques et informatiques. Le maintien de la viabilité infrastructurelle ne se réduit pas à la seule maintenance du protocole, comme le visibilise la crise précédente, loin s'en faut. Si notre intérêt partira des crises protocolaires, n'oublions pas que, en tant qu'infrastructure, une CM se décompose en différents sous-systèmes articulés, mobilisant des composantes et des interactions à la fois *au sein de la chaîne** et en *dehors de celle-ci* : Bitcoin et Ethereum sont des mille-feuilles d'acteurs, d'arrangements et de dispositifs hétérogènes, et leurs propriétés de sécurité, de stabilité et de confiance relèvent d'une multi-dimensionnalité où le technique, le légal, le réglementaire et le socio-économique s'enchevêtrent (cf. Chap. I, section I.2). Bitcoin et ses parties prenantes sont ainsi exposés à des risques et crises pouvant revêtir des formes très différentes.

Une CM et sa communauté peuvent être ébranlées par des crises affectant non seulement le protocole de la CM, mais aussi tout autre composant et domaine participant de leur infrastructure. Pour utiliser une CM, l'usager fait d'emblée face à sa dimension infrastructurelle et, à chaque étape ou couche, peut voir s'installer le bogue ou l'attaque informatique : il doit mobiliser une machine (ordinateur ou téléphone), avoir un accès internet, un navigateur et d'autres applications tierces médiatisant ses interactions *on chain*, et chacun peut être dysfonctionnel ou avoir été compromis. Chacun des quatre domaines de sécurité informatique distingués dans le champ de la science informatique (Lee 2019, p. 38-39, Figure 11 suivante) peut connaître des crises, renvoyant à 6 grandes familles de menaces et 17 risques de sécurité associés (*Ibid.* p.34-36)³⁶¹.

Figure 11 : Les quatre grands domaines de crise



1- Domaine des points finaux, correspondant à l'ensemble des éléments machines (dit « *hardware* ») dont l'usager a besoin afin d'interagir avec le protocole ou avec les interfaces clients en question (ordinateurs et mobiles, portefeuilles* physiques, terminaux de paiement, etc.).

2- Domaine des interfaces client, renvoyant à l'ensemble des éléments logiciels (dit « *software* ») servant d'interface entre l'usager et le protocole (application tierce et leur « *front end* », cf. interfaces de plateforme d'échange, de DEX et autres « *Dapp* », etc.).

3- Domaine des applications distribuées, renvoyant à l'ensemble des

³⁶¹ À la granularité académique très fine de Lee (2019, p.37 et 61-64), nous avons préféré pour la suite nous en tenir aux labellisations indigènes que nous avons rencontrées, et que cette section vise à présenter.

scripts à exécution programmatique (cf. *Smart Contract*^{*}) mobilisés et qui peuvent contenir des vulnérabilités ou avoir été économiquement mal conçus.

4- Domaine des protocoles de registre distribué, couvrant l'ensemble des éléments constitutifs du protocole de registre^{*} distribué, qu'ils relèvent de la couche protocolaire, de la couche réseau^{*} P2P ou de la couche base de données (cf. Annexe n°V.6).

Bien que chaque domaine puisse entrer en jeu et/ou participer d'une crise de CM, suivant le tropisme des *bitcoiners*^{*}, notre attention s'est portée spécifiquement sur les crises Bitcoin relevant du domaine du protocole de registre^{*} distribué. Aucune volonté de minimiser les conséquences importantes sur l'écosystème et la valeur d'échange de l'UCN^{*}, que les réglementations et annonces légales, les attaques et vols de plateforme d'échange, perte/vol individuel, arnaques, exploitation de vulnérabilité dans des SC, peuvent induire (en témoigne notre chronologie du chapitre I). Mais nous avons voulu cibler l'objet central des *coiners*^{*}, pour qui les domaines non protocolaires n'ont pas en soi de pertinence, du fait justement qu'ils renvoient à un ailleurs protocolaire duquel ils se revendiquent autonomes. De cette manière, cela permettait d'interroger frontalement les CM et leur communauté sur les conditions nécessaires au maintien de la sécurité, des propriétés fonctionnelles désirées et de la confiance qui leur est accordée.

Enjeux des crises Bitcoin : labélisations indigènes et exemples historiques

Nos recherches sur le Bogue CVE 2018 #17144 nous ont conduit à mettre au jour le nombre important de crises protocolaires que Bitcoin et sa communauté ont eu à essuyer. Une requête en ligne associant les mots « Bitcoin », « CVE », « vulnerability » nous fit rencontrer une base de données tenue par des volontaires, sous forme d'un wiki Bitcoin communautaire³⁶², où est consigné l'ensemble des bogues protocolaires Bitcoin (c'est-à-dire perçus comme tels). La réalisation de la chronologie suivante et le défrichage netnographique associé nous confrontèrent au fait que traiter des crises, c'est d'abord traiter les marques de leur fabrication et de leur gouvernance. Nous avons découvert des documents d'information, des acteurs, des dispositifs, des lieux et arènes hétérogènes. Ces documents et le jargon usité (« *affect* », « *severity* », « *attack is..* », « *flaws* », « *fix* », « *fix deployment* », voir Bitcoin Wiki) déployait des distinctions entre types de failles, associés à des dispositifs d'informations/publicisation, des catégories et labélisations (comme CVE ou BIP), des dates d'annonce pas forcément publique, des informations concernant les implémentations logicielles (« *wxBitcoin* », « *bitcoind* », « *Bitcoin-QT* ») et les versions affectées et corrigées (0.3.4 ;0.3.5, etc.), l'établissement de niveaux de sévérité, de procédures de résolution, etc. Le numéro d'identification CVE renseigne sur le fait que les *bitcoiners*^{*} ont intégré à leur infrastructure des artefacts existants, en l'espèce la procédure d'étiquetage/publicisation normalisée du système « *Common Vulnerabilities & Exposures* » (ou CVE). Ce système suppose la mise à disposition d'une base de données publique contenant une référence publique, une date et un numéro d'identification, qui doit permettre de reporter, d'annoncer, de référencer, donc d'informer le public des failles de sécurité informatique³⁶³. Ce système étant ancien et généralement utilisé dans le développement informatique, les *bitcoiners*^{*} ont ajouté une labélisation *ad hoc*, mieux taillée pour leur besoin, qu'ils mobilisent conventionnellement (Tableau 4 suivant, *Ibid.*).

³⁶² Voir https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures [consultation au 20/10/2021].

³⁶³ Voir <https://nvd.nist.gov/vuln/detail/CVE-2018-17144#VulnChangeHistorySection> [consultation au 20/10/2021].

Tableau 4 : Labérisation indigène des vulnérabilités de Bitcoin

Label « indigène »	Définition
Scission du réseau* « Netsplit »	L'unicité du réseau* et du registre* canonique est remise en cause : apparition d'un ou plusieurs réseau*(x) différent(s), avec des nœuds* travaillant sur des historiques de transactions* différents, sans convergence possible.
Attaque par Déni de Service « DOS »	L'accès au réseau* est plus ou moins perturbé, des nœuds* rencontrant des problèmes (crash, difficulté de traitement des données entrantes, etc.).
Vol « Theft »	Un ou plusieurs acteur(s) peu(ven)t prendre le contrôle d'UCN* en dehors des règles protocolaires consensuelles.
Faux monnayage « Inflation »	Un ou plusieurs acteur(s) peu(ven)t créer des UCN* en dehors des règles de monnayage protocolaire canonique.
Exposition « Exposure »	Un ou plusieurs acteur(s) peu(ven)t accéder à des données d'un ou plusieurs utilisateur(s) en dehors de ce qui est conventionnellement prévu.
Inconnue « Unknown »	L'étendue des abus potentiels n'est pas connue précisément.
Fausse confirmation « Fake Conf »	Un ou plusieurs acteur(s) peu(ven)t réaliser des doubles dépenses avec une confirmation*.
Tromperie « Deception »	Un ou plusieurs acteur(s) peu(ven)t propager des informations erronées au sein du réseau*.

Source : Rolland Maël

Construite pratiquement, cette labérisation permet de catégoriser l'ensemble des bogues/failles passés ou futurs de Bitcoin. Chaque label dessine les frontières de grands types de crises protocolaires et des actions pathologiques induites. Pour chaque crise, les *bitcoiners** ajoutent à ces labels des informations concernant le degré de gravité (« *easy* », « *hard* », « *very hard* ») et/ou des acteurs concernés (« *miners* », « *Keyholders* », « *RPC access* », etc.). Cet étiquetage permet de caractériser et de publiciser les différents bogues et d'en informer l'ensemble des membres de la communauté. Cette normalisation indigène constitue le fond et la forme des crises répertoriées, qui a servi de matériau à la réalisation de la chronologie que nous avons construite.

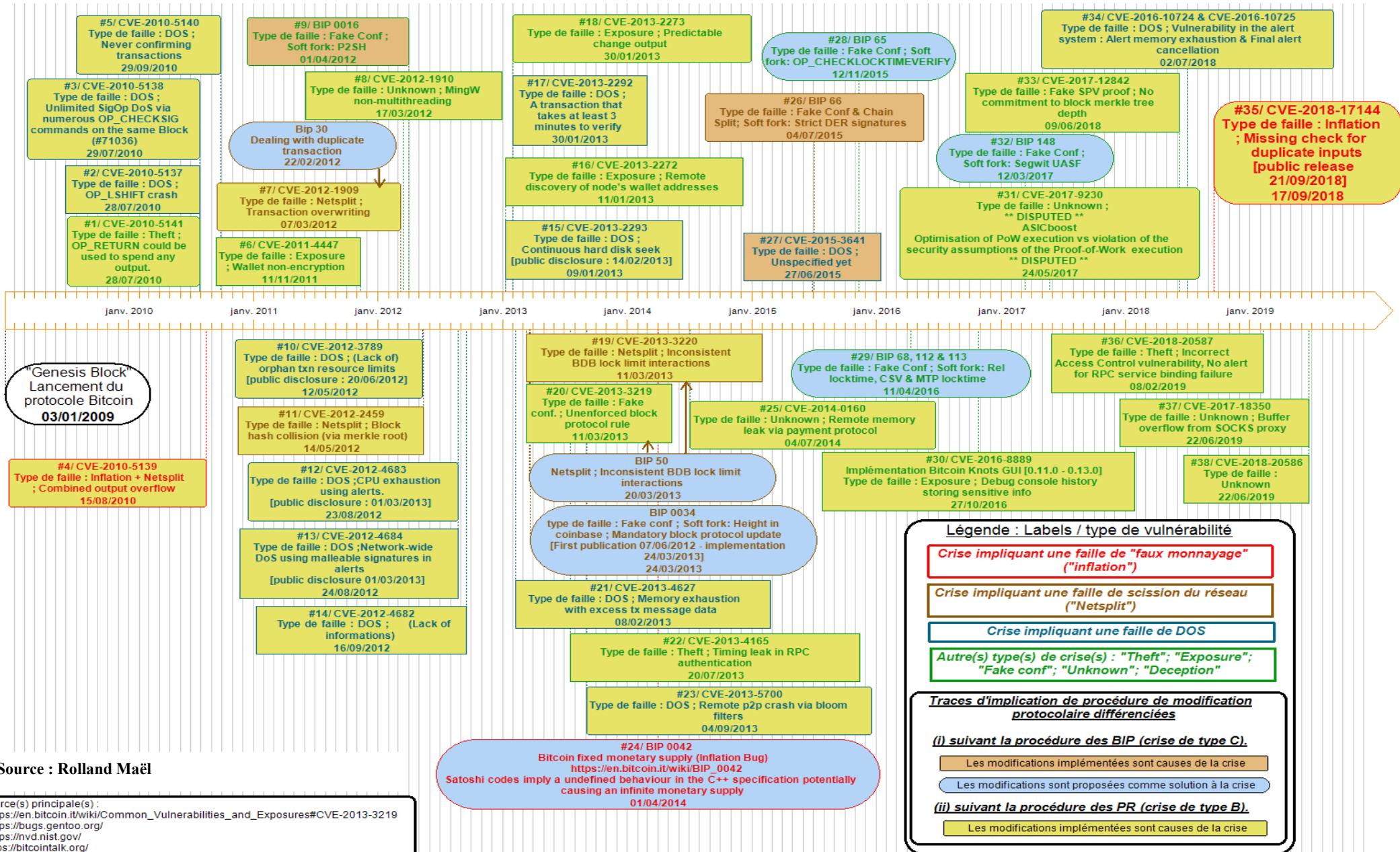
Grâce aux données de Bitcoin Wiki croisées avec d'autres sources, nous avons répertorié³⁶⁴ pas moins de 38 crises entre 2009 et la fin 2019 (cf. Chronologie 4 suivante). Chaque crise répertoriée est représentée par un rectangle contenant, de haut en bas : (i) un identifiant, renvoyant à deux systèmes d'identification différents, présentant soit le numéro CVE de la vulnérabilité, soit celui du « BIP » impliqué dans la survenue et/ou la résolution du problème, ces deux types d'identification pointant une distinction franche entre deux familles génériques de crise et l'existence concomitante de procédures de résolution différencierées (cf. code couleur); (ii) le type de crise, en suivant la labélisation indigène constituée de 8 labels (cf. section prochaine) permettant de couvrir l'ensemble des risques de vulnérabilité protocolaire potentiels, auquel (iii) nous ajoutons des informations les concernant ; enfin, (iv) la date de divulgation publique d'abord, si elle ne coïncide pas avec la date de la première divulgation (privée). Cette dernière est toujours présentée en dernier et conçue comme date de déclenchement effectif ; les deux dates éclairent sur la durée, parfois prolongée, des actions correctives entreprises, pendant laquelle la communauté n'a pas d'information les concernant. Étant donné la faible diversité logicielle sur Bitcoin, nous n'avons pas listé les différentes implémentations et versions affectées. Nous avons pour finir utilisé un code couleur³⁶⁵. L'encadrement du texte vise à différencier les labels/types de vulnérabilité au cœur de nos cas d'étude de ceux qui y sont étrangers, regroupés ensemble : encadrées en rouge, les crises induisant un risque de « faux monnayage » (ou « *inflation* », il y en a 3); en marron, les crises induisant un risque de scission du réseau* (« *Netsplit* », il y en a 4) ; et en bleu, celles induisant un risque de DOS (elles sont au nombre de 13). Celles restantes (« vol », « exposition », « inconnue », « fausse confirmation* », « tromperie ») ont été regroupées, en vert.

La couleur du fond encadré souligne quant à elle les procédures de modifications protocolaires impliquées (dans l'insémination ou la résolution) des vulnérabilités : en cas d'implication de la procédure appelée BIP, pour « *Bitcoin Improvement Proposal* » (cf. section n°I.2.3 suivante), le fond bleu clair indique que la vulnérabilité a été introduite par un BIP (comme cela s'est produit 3 fois), là où le fond orange foncé dénote au contraire que c'est la résolution (« *FIX* ») qui est passée par cette procédure (les flèches précisant le lien entre la faille et son BIP de résolution). Dans le cas inverse, c'est la procédure des « *Poll request* » qui est impliquée, soit dans la mise en crise, soit dans la résolution (en jaune, comme ce fut le cas de la crise Bitcoin CVE 2018). Cet ensemble va nous permettre de mettre en perspective les enjeux de la crise CVE 2018.

³⁶⁴ Ce recensement ne prétend pas à l'exhaustivité. Tout d'abord, car certaines crises ont un statut controversé, comme c'est le cas de la crise n°31/ CVE-2017-9230 concernant l' « ASICboost » : pour certains, cette méthode de traitement des transactions* dans la production des enregistrements correspond à une violation des hypothèses de sécurité posées par Nakamoto [Anon , Entretien n°3] ; pour d'autres, c'est une méthode qui, bien que non envisagée à l'origine, est possible, d'où son absence sur le site https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures, [consultation au 29/10/2021]. Ensuite, en vue de simplification et suivant la circonscription de nos terrains, notre recensement est limité aux vulnérabilités affectant le protocole Bitcoin et ses logiciels canoniques, celles affectant le protocole « Lightning Network » ou les logiciels et services tiers ayant été laissées de côté.

³⁶⁵ En cas d'itérations multiples de faille, la couleur renvoie à la gravité la plus élevée. Par exemple, la crise n°26 labélisée « *Fake conf* » a failli causer une « scission de chaîne » (Light 2019), d'où l'utilisation du marron.

Chronologie 4 : Bitcoin, une histoire rythmée de crises à gérer



Crise de « faux monnayage », ou l’immutabilité des règles de monnayages en question

Les bogues portant l’étiquette « inflation », bien que rares (3 recensés, crises n° 4, 24 et 35, en rouge dans notre chronologie), sont particulièrement critiques. Ils touchent à la confiance éthique et hiérarchique en remettant en cause l’« immutabilité » et la prévisibilité du monnayage comme des règles transactionnelles : leur présence introduit un doute sur le fait que l’offre monétaire suive les modalités d’émission reconnues comme canoniques, puisque des UCN* peuvent être émises en dehors des limites protocolaires. Du fait de leur gravité, ces bogues représentent l’une des principales préoccupations des développeurs*, qui doivent tout « faire pour que le système Bitcoin fonctionne comme attendu par les utilisateurs, c'est-à-dire que la masse monétaire soit limitée à 21 millions d'unités, que personne ne puisse imprimer de l'argent, toutes ces choses standards que l'on peut souhaiter, hehehe [cela le fait sourire], avec [...] Bitcoin » [M. Corallo ; entretien n° 15]. Historiquement, « ce n'est pas la première fois que Bitcoin est vulnérable à l'inflation mais, hum [...] c'est la première depuis Satoshi » [M. Corallo ; entretien n° 15]. La crise CVE 2018 #17144 est même, suivant notre décompte, la troisième occurrence de ce type de crise et la deuxième depuis le départ de son/ses créateur(s). Mais seule la première a conduit à l’émission effective d’UCN* en dehors des règles de monnayage qu’aurait fixées Nakamoto.

La première crise de faux monnayage dont parle Corallo est la faille CVE 2010 #5139 (crise n° 4) d’août 2010, communément appelée « *Bitcoin bug Value Overflow* ». Arrivée dans l’enfance de Bitcoin, c’est S. Nakamoto et les premiers développeurs* qui se chargeront de la remise en ordre. Le 15 août, un « *enregistrement étrange* [, le] 74638 »³⁶⁶ est pointé par J. Garzik sur *Bitcointalk*. Les *bitcoiners** présents échangent leurs analyses. Ce bloc aurait subi « *un débordement d’entier* » (« *integer overflow* ») où la « *somme des deux sorties déborde sur un négatif. C'est un bug dans les contrôles de transaction** qui ne l'ont pas rejeté, puis quelqu'un l'a remarqué et l'a exploité. On peut supposer qu'une nouvelle version sera en mesure de la rejeter et de lancer un nouveau Fork* valide. » (« *Ifm* »³⁶⁷). Bien au-delà du cap des 21 millions d’UCN*, l’exploitation en crée plus de 184 milliards. Pour les acteurs, le code fautif n'est pas loi, les résultats qu'il produit sont « *un sérieux problème* » (« *Theymos* »³⁶⁸), expliquant une remise en ordre réalisée en quelques heures et mobilisant la grosse artillerie. G. Andresen rend un premier correctif « *disponible avant le réveil de Satoshi* » (« *myzerydearia* »³⁶⁹), « *jusqu'à ce qu'il y ait une meilleure solution...* »³⁷⁰. Dès la découverte du problème, Nakamoto s’attèle au correctif. S’il publie rapidement un « *changement préliminaire* », il a « *d'autres changements à faire* »³⁷¹ et, pour gagner du temps, il enjoint les mineurs à stopper leurs opérations. L’utilisateur « *imf* » l’a anticipé, la solution est de faire un *Fork**, « *refaire une branche autour de la branche actuelle* », aussi « *cela aiderait si les gens arrêtaient de générer [de nouveaux blocs, NdA]* » car « *moins vous générerez, plus vite ce sera fait* »³⁷². La remise en ordre suppose de remplacer/supprimer l’enregistrement pathologique du registre* canonique en le rendant orphelin (cf. chap. I) afin de revenir dans le temps des enregistrements. La solution implique le développement et la publication d’une version logicielle corrigée (la v0.3.10³⁷³) et que les opérateurs de nœuds* (mineurs ou complets) se mettent à jour et

³⁶⁶ Voir le post original et la discussion ouverte ici : <https://bitcointalk.org/index.php?topic=822.0>, qui s'est ensuite reportée sur le fils du forum des développeurs*, là : <https://bitcointalk.org/index.php?topic=823>, (consultation au 02/11/2021).

³⁶⁷ Voir <https://bitcointalk.org/index.php?topic=822.msg9487#msg9487> [consultation au 02/11/2021].

³⁶⁸ Voir <https://bitcointalk.org/index.php?topic=822.msg9481#msg9481> [consultation au 02/11/2021].

³⁶⁹ Voir <https://bitcointalk.org/index.php?topic=822.msg10348#msg10348> [consultation au 02/11/2021].

³⁷⁰ Voir <https://bitcointalk.org/index.php?topic=823.msg9524#msg9524> [consultation au 02/11/2021].

³⁷¹ Voir <https://bitcointalk.org/index.php?topic=823.msg9530#msg9530> [consultation au 02/11/2021].

³⁷² Voir <https://bitcointalk.org/index.php?topic=823.msg9531#msg9531> [consultation au 02/11/2021].

³⁷³ Voir <https://bitcointalk.org/index.php?topic=827.0> [consultation au 03/11/2021].

remplacent leurs versions locales du registre* pour une version d'« *avant le bloc 74000* ». Dans ce cas, ce n'est pas le consensus de Nakamoto en PoW* qui « *résout le problème de la détermination de la représentation dans la prise de décision à la majorité* » (Nakamoto 2008c, p. 3), mais l'homme Nakamoto qui fait consensus autour de son correctif, grâce à une coordination à l'opposé de « *minimale* » (*Ibid.*, p. 8) : la convergence de tous les nœuds* sur un historique ne contenant pas l'émission surnuméraire ne passe pas par l'application automatique d'un consensus technique, elle se fait contre lui, par consensus social et coordination *off chain**, « *environ cinq heures après l'incident [...] avant que la « bonne » chaîne ne reprenne la tête du PoW** ». Bien que d'autres le contestent (Bitmex Research 2017a), la remédiation de cette crise est conçue par certains *coiners** comme une remise en ordre de type « *RollBack* » (Dino Mark, cité par Shin 2022, p. 144), un type de modification protocolaire hautement problématique pour une CM et les *coiners** les plus rigoristes, car il correspond à une remise en cause du principe de l'inviolabilité des données endogènes* consignées dans la chaîne (cf. section III.3.). Cette crise est la seule à avoir conduit effectivement à sortir, pour un temps, du cadre de monnayage reconnu de tous les *bitcoiners**.

Ce que ceux-ci savent moins, c'est que ce cadre et le cap des 21 millions d'UCN* bitcoin, *soi-disant* fixés dans le marbre dès l'origine, Nakamoto, faillible, l'avait mal programmé à l'origine, et il ne fut effectivement « fixé » dans le code qu'en 2014, à l'occasion de la seconde crise étiquetée « faux monnayage ». Elle renvoie au « *Bitcoin Improvement Proposal #0042* » (crise n°24) d'avril 2014, qui la corrigera. Latente, cette vulnérabilité n'a pas conduit à une émission surnuméraire, mais, sur le temps long, elle y conduisait programmatiquement. En effet, les codes de Nakamoto visant à fixer la limite des 21 millions d'UCN* étaient défaillants, sans que personne n'y ait jamais prêté attention. La propriété la plus vantée des *bitcoiners** dut attendre près de 5 ans après le lancement de Bitcoin avant d'être réellement implémentée dans ses codes logiciels, en 2014. L'erreur fut découverte par P. Wuille, qui joint à l'annonce publique une proposition de remédiation, sous la forme du BIP n°0042. Pour coller à l'énormité de l'erreur, le tout est réalisé le 1^{er} avril, avec un ton volontairement humoristique³⁷⁴ : « *bien que l'on pense généralement que Satoshi était un goldbug détestant l'inflation, il n'a jamais dit cela et a en fait programmé la masse monétaire du bitcoin pour qu'elle augmente indéfiniment, pour toujours. Il a modélisé la masse monétaire comme 4 mines d'or découvertes par millenium (1024 ans), avec des intervalles égaux entre elles, chacune étant épuisée au cours de 140 ans.* »³⁷⁵ L'erreur qui devait conduire à ce que de nouveaux cycles d'émission de 21 millions d'UCN* « *recommence[nt] tous les 250 ans* » repose sur une erreur d'utilisation du langage C++ (« *the code was just illegal C++* », P. Wuille³⁷⁶). Renvoyant à un temps long (140 ans), excédant la vie d'un individu ; la corriger ne semblait pas controversé, d'où l'ironie de Wuille qui dit proposer « *un changement controversé : rendre l'offre monétaire de Bitcoin limitée* »³⁷⁷.

La faille Bitcoin CVE 2018 est la troisième occurrence d'une crise de ce type, et sa singularité tient à ce que le risque de production d'UCN* surnuméraires résidait, nous l'avons vu, dans les mécanismes entourant la double dépense et non ceux entourant les récompenses, comme les crises précédentes. Précisément, l'itération de « faux monnayage » concerne les versions « Bitcoin Core »

³⁷⁴ N'étant pas technicien, nous sommes d'abord passé à côté de cette ironie, d'où l'épisode, déjà rappelé en note dans l'introduction générale, d'un *bitcoiner** français contestant l'existence de ce bogue, affirmant que nous étions tombé dans un poisson d'avril (voir <https://twitter.com/daboloskov/status/1246527105627635713?s=20> et suivant). Luke Dash Jr, P. Wuille et M. Corallo nous en ont confirmé la véracité.

³⁷⁵Voir https://en.bitcoin.it/wiki/BIP_0042 [consultation au 03/11/2021].

³⁷⁶ Voir <https://twitter.com/pwuille/status/1246564993400635395?s=20> [consultation au 03/11/2021], cette « illégalité » fait référence aux normes d'usage du langage de programmation* C++, comme m'en a informé Anon n°4 [Entretien n°10].

³⁷⁷ Voir https://en.bitcoin.it/wiki/BIP_0042 [consultation au 03/11/2021].

0.15 à 0.16.2 qui considèrent valide un enregistrement, pourtant « invalide » du point de vue des clients non vulnérables (cf. cas D, Tableau 2). Cette transgression des règles contourne le monnayage et ses mécanismes d'émission, les UCN* doubles dépensées sont doublement comptabilisées, créant « *des BTC à partir de rien* » (Song 2018).

En pratique, en plus d'une augmentation discrétionnaire/arbitraire de la masse monétaire de bitcoin, l'activation de ce bogue aurait entraîné un autre risque important pour toute CM : une « scission de chaîne » (un « *chain split* »).

Crise de « scission de chaîne » : l'unicité des paiements mise en péril

Comme les bogues de faux monnayage, les « scissions de chaîne » (ou « *chain split* ») sont rares (4 recensées, crises n°7, 11, 19 et 26, en marron) et, comme eux, leurs conséquences sont critiques. Elles peuvent en effet causer un effondrement de la confiance éthique, hiérarchique, mais aussi méthodique. Alors que la situation normale est celle d'une unicité du réseau* et du registre, ces crises impliquent que le protocole et le réseau* se scindent en deux ou plusieurs versions concurrentes, sans que le consensus par PoW* de Nakamoto soit capable de faire converger les nœuds* sur un historique unique. L'établissement de frontière nette entre le normal et l'anormal n'est jamais donnée en soi et évolue au gré des interprétations : souvenons-nous que la cohabitation à un instant t de deux historiques n'est pas pathologique en soi. En temps « normal », en cas d'occurrence de deux enregistrements candidats valides, la règle stipulant aux nœuds* de converger vers la chaîne la plus longue permet une réconciliation rapide de l'ensemble du réseau* sur un même registre* canonique, par réorganisation de chaîne (cf. Chap. I) : le consensus par PoW* ne peut fixer techniquement une norme de finalité des transactions*, celle en vigueur, établie à 6 cycles de mise à jour du registre* (*dit confirmation**) est une convention de pratique³⁷⁸.

En cas de « scission de chaîne », le consensus de Nakamoto échoue, car une incompatibilité logicielle empêche la réconciliation entre des nœuds* aux règles divergentes : le réseau* de paiement s'est séparé en deux mondes clos. Ces situations renvoient originellement à des situations d'indomptabilité involontaire³⁷⁹. Pour qu'une scission de chaîne advienne, il suffit qu'un « *bug [...] dans une nouvelle version du logiciel fasse qu'une transaction* est considérée comme valide [là où l'ensemble des autres] la rejette comme non valide. [...] Seul le sous-ensemble des participants qui ont mis à jour leur logiciel [l']acceptera [et] comme les transactions* et les blocs sont enchaînés, les deux sous-ensembles seront en désaccord sur chaque transaction* qui suivra. Sans une action rapide des développeurs* et une campagne [off chain*] visant à aligner tous les participants d'un côté ou de l'autre de la scission, les deux camps [...] ne pourront plus jamais se mettre d'accord [,] la monnaie [est] divisée en deux monnaies incompatibles* » (Fields 2018). Dans une telle situation, le « *timing joue un rôle crucial* ». La difficulté de résolution dépendra de la gravité de la situation et de son évaluation : « *si la chaîne est divisée de telle sorte que 99% des participants sont d'un côté et seulement 1% de l'autre, se ranger du côté de la majorité est la solution évidente. Cependant, si environ 50% des participants sont passés à la nouvelle version, il n'y a pas de choix facile.* » (Ibid.)

³⁷⁸ Rappelons que les « *attaques 51%* », visant à créer des doubles dépenses, correspondent à une situation où un acteur en capacité de produire des enregistrements rapidement détourne à son profit cette dimension transitoire et sa définition conventionnelle, produisant en privé une chaîne d'enregistrement concurrente, qu'il publiera en temps voulu afin que l'ensemble du réseau converge vers son historique et annule les transactions qu'il a inscrites dans la chaîne ainsi rendue orpheline (cf. Annexe n°V.5).

³⁷⁹ L'intentionnalité dessine le cas particulier des « *Hard Forks contentieux* » où un groupe monétaire différencie ces codes pour s'autonomiser de sa communauté de paiement d'origine (cf. « *Scaling Debate* », Chap. II section II.3.3 et section II.3.3, suivante).

Si ces solutions apparaissent évidentes pour les 99% il n'en est sûrement pas de même pour ceux qui font partie du 1%.

Avec une coordination technique mise en défaut, le consensus *par* le protocole n'implique aucun retour à la normale, et la seule remise en ordre possible relève d'une coordination sociale, une action coopérative et « *off chain** » entre les opérateurs de noeuds* (mineurs et complets). Ce type de coordination suppose des négociations entre opérateurs, car cette convergence forcée a des enjeux économiques importants pour les participants à la chaîne minoritaire rendue orpheline : les transactions* qui y sont consignées - les échanges économiques des usagers et les subsides des mineurs – n'ont plus d'existence une fois la réconciliation advenue, ce qui n'est pas le cas des contreparties de ces transactions* engagées dans les échanges. Les crises historiques qui ont impliqué des « scissions de chaîne » ont bien conduit à l'« *action rapide des développeurs** et [à des] campagnes visant à aligner tous les participants » (Fields 2018) sur la même branche. La gravité de ce type d'événements est réelle ; ils dégradent l'expérience des usagers et peuvent conduire à des pertes pécuniaires : durant ces crises, avoir accepté des transactions* revient à encourir le risque de doubles dépenses, avec de mêmes UTXO* dépensées dans chacune des branches concurrentes (cas de la crise n° 19 de 2013) et des annulations de paiements confirmés (lorsque la scission se termine et que tous les noeuds* convergent sur un même historique, rendant orphelin l'historique concurrent). D'où la création d'outils d'observation et d'analyse, un site comme « Fork*Monitor.info » mis à disposition par « BitMEX research » monitorant en temps réel l'occurrence de deux enregistrements candidats valides comme la présence ou non de tentative de double dépense, ou d'augmentation de frais de transaction*. La gravité de ces crises s'apprécie finalement aussi par les voies correctives utilisées, et les remises en ordre passent souvent par des BIP (BIP 30, 0034 et 50).

Le « Bug Value Overflow » (crise n° 4, CVE 2010 5139) est un cas de « scission de chaîne ». L'apparition de l'enregistrement à émission surnuméraire a produit une séparation du réseau* entre les noeuds* acceptant cet historique et ceux le refusant. La scission fut longue de 51 blocs, avant que la « chaîne légitime », au sens des attendus sociaux, réclame sa victoire en termes de PoW*, grâce au travail de remise en ordre coordonné de Nakamoto, Andresen et Garzik, (Redman 2021). La crise n° 19 (CVE 2013 #3220), déclenchée en mars 2013, illustre tant la gravité des problèmes posés que la coordination nécessaire (c'est l'une des controverses analysées par Musiani, Mallard et Méadel 2018, p. 138 à 142) : « *les 11 et 12 mars 2013, un mineur exécutant la version 0.8 [...] a créé un gros bloc invalide [conduisant à] une scission ou une "bifurcation" involontaire dans la blockchain Bitcoin, puisque les ordinateurs équipés de la version la plus récente du logiciel à l'époque (0.8) ont accepté le bloc invalide et ont continué à construire sur la chaîne divergente, tandis que les anciennes versions du logiciel l'ont rejeté et ont continué à étendre la blockchain ancienne/original sans le bloc incriminé. Cette scission a entraîné la formation de deux journaux de transactions* distincts sans consensus clair ni même connaissance de l'existence de l'autre événement, ce qui a permis aux mêmes fonds d'être dépensés deux fois sur chaque chaîne - l'acte même de double dépense dont l'évitement était censé être la principale amélioration du bitcoin par rapport aux monnaies numériques précédentes* » (*Ibid.*). Cette crise, plus courte, avec seulement 21 blocs rendus orphelins (Bitmex Research 2017a; Redman 2021), fut malgré tout plus controversée que la précédente. Sa résolution a reposé sur une coopération active entre les développeurs* et les pools de minage, qui permit la remise en ordre en alignant « *tous les participants d'un côté ou de l'autre de la scission* » (Fields 2018) et ce, en dehors du consensus de Nakamoto : une pool de minage importante est revenue à la version logicielle antérieure afin de suivre l'historique défini socialement comme canonique.

Pour le bogue Bitcoin CVE 2018 que nous étudions, seule l'absence d'exploitation effective justifie que l'étiquette de « scission de chaîne » ne lui ait pas été assignée. Un bloc contenant une transaction* réalisant une double dépense eut été accepté par des nœuds* et rejeté par d'autres, nous aurions été dans le cas extrême décrit par Fields (2018). Les versions 0.15.0 à 0.16.2 acceptant l'enregistrement « pathologique » comme canonique auraient étendu la chaîne d'enregistrement à partir du bloc avalisant la double dépense et les « nouvelles » règles transactionnelles et de monnayage, là où les nœuds* tournant sur des versions non vulnérables l'auraient rendu « orphelin », continuant à travailler sur un registre* au sein duquel les transactions* sont valides du point de vue des « anciennes » règles. L'exploitation de cette vulnérabilité sur le réseau* testnet de Bitcoin quelque mois après, profitant du fait que « certains mineurs étaient encore vulnérables » le prouve (Straw Hat 2019) : « *boom, le réseau* s'est divisé* » [...] « *pendant des heures* » avant qu'un acteur active « *une puissance de hachage importante* [...] afin de reconstituer quelques centaines de blocs et de réorganiser la chaîne honnête » (Straw Hat 2019). Reste que, dans le cas de la crise Bitcoin CVE 2018, la gravité théorique de ce bogue est nuancée par ses conditions pratiques. Song (2018) et Straw Hat (2019) soulignent qu'exploiter cette vulnérabilité n'est offert qu'au producteur d'enregistrement. Cela implique des coûts (directs et d'opportunités) importants, pour ne pas dire rédhibitoires (aux dépenses afférentes à la découverte d'un hash* valide s'ajoute la perte de 12,5 BTC de récompense, Song 2018). Au capital économique nécessaire s'ajoute un capital culturel de haut niveau (savoir et savoir-faire dans la programmation de Bitcoin)³⁸⁰. Finalement, à l'époque, si près de 82,5% du réseau* était vulnérable au bogue CVE 2018 #17144 (4,3% à l'itération DOS et 78,3% pour celle de « faux monnayage », Tableau 3 ci-dessus), près de 17,5% des nœuds* du réseau* n'étaient pas concernés par cette vulnérabilité. En cas de « *bifurcation de chaîne* », « *le consensus social [...] concernant la bonne chaîne aurait commencé à être discuté et la chaîne créant une inflation inattendue aurait probablement perdu. S'il y avait eu un blocage, il y aurait probablement eu un retour en arrière volontaire pour punir l'attaquant.* » (Song 2018) Difficile, en l'absence d'exploitation effective, de savoir la tournure qu'aurait prise cette crise en cas de « scission de chaîne » (Song 2018), d'où l'intérêt de l'expérience de Straw Hat (2019) sur le testnet Bitcoin.

Crise de « DOS » : dégradation de l'accessibilité au réseau et de la praticité des paiements

Les vulnérabilités de déni de service (DOS) sont les plus fréquentes (13 décomptées ; crises n° 2, 3, 5, 10, 12, 13, 14, 15, 17, 21, 23, 27 et 34 ; en bleu) mais moins critiques, en ce qu'elles n'impliquent qu'une érosion de la confiance méthodique : seule la praticité des paiements est remise en cause, du fait de la congestion du réseau*. S'en prémunir est nécessaire afin que le réseau* soit accessible et disponible à tous, et les problématiques entourant leur régulation sont au cœur du design des protocoles de registre* distribué. En outre, toute « attaque » DOS n'est pas due à la présence d'un bogue « à proprement parler » (cf. les cas recensés dans notre chronologie). La dimension normative et politique supportant la normalisation des frontières du phénomène ressort ici. Bitcoin a été la cible de nombreuses « tempêtes » de spam (Lopp 2021 en a décompté 14, étaillées entre 2011 et 2021). Celles-ci ont contribué à faire évoluer les régulations protocolaires encadrant des « *transactions* de spam* » qui « *d'un certain point de vue [...] n'existent pas - si elles sont valides et qu'elles paient les frais appropriés, elles doivent être confirmées* » (Lopp 2021; la taille

³⁸⁰ L'utilisateur moyen est exclu, car créer cette transaction exige de tout faire manuellement, en lignes de commande via un client mineur. Utiliser un client de portefeuille* est impossible, car il l'empêcherait par défaut. Si certains considèrent qu'un bon *bitcoiner/coiner** ne peut « *comprendre Bitcoin* » que s'il a « *construit une transaction [...] avec [se]s mains [...] avec du code* » [P. Noizat, Entretien n°24], notre expérience démontre que ces compétences sont rares chez les *bitcoiners**, et l'expérience de *Straw Hat* (2019) confirme le haut degré de spécialisation et d'expérience nécessaire.

des blocs à 1 Mo, le mécanisme des frais de transaction* et des frais relais, cf. Chap. I, section I.2.1). À leur fréquence renvoient des effets relativement peu critiques, puisqu'une crise de DOS n'est que transitoire et partielle, ne touchant que certains acteurs.

Tout d'abord, « *si le nœud* Bitcoin de quelqu'un se déconnecte [...] dans la plupart des cas, vous ne perdrez pas d'argent [simplement,] vous ne pouvez pas accepter un paiement, c'est nul pour votre entreprise mais au moins vous n'avez pas perdu d'argent.* » [M. Corallo, Entretien n°15] Ensuite, pour les DOS de « *tempêtes de spam* », bien qu'incommodes, elles se régulent par le mécanisme même qu'elles attaquent, celui des frais de transaction* : « *remplir la "mempool" avec un grand nombre de transactions* crée une plus grande compétition pour l'espace des blocs, ce qui augmente les frais requis pour une confirmation* plus rapide.* » (Lopp 2021) Ces situations de crise impliquent des problèmes de synchronisation des nœuds* et de latence, perturbant la disponibilité* et la vivacité du réseau* P2P pour certains acteurs seulement³⁸¹. Comme l'illustre l'itération « *DOS* » de la faille Bitcoin CVE 2018 concernant les versions 0.14 à 0.14.3 (non incluse) des implémentations « *Bitcoin Core* » (Bitcoin Core 2018 ; Song 2018 ; Awemany 2018) qui permettait d'« *appeler le nœud* à planter, si* » un mineur diffusait un enregistrement pathologique pour faire planter les pairs qui le réceptionneraient : appliquant leur règle canonique de validité des enregistrements, le bloc ne serait pas accepté et le nœud* planterait/s'arrêterait. La distribution du réseau* se fait garante d'un accès minimum, des nœuds* non vulnérables continueront le traitement et la maintenance du registre* en l'absence des autres. Reste une expérience usagers qui se dégrade, c'est plus cher et la finalité du paiement est incertaine³⁸² [A. Le Calvez, Entretien n° 20].

D'autres types de crises passées et encore à découvrir

D'autres types de vulnérabilités peuvent exister et leur gravité (et leurs conséquences en termes de confiance) s'apprécie à leur caractéristique idiosyncratique. Les vulnérabilités de type « *Theft* » sont rares (au nombre de 4 ; crises n° 1, 22, 36 et 39), mais critiques, renvoyant à des situations où un attaquant peut prendre le contrôle d'UTXO* en dehors des règles consensuelles canoniques (cf. avoir la bonne signature). Heureusement pour la sécurité de Bitcoin – et plus particulièrement pour la perception qu'en ont les utilisateurs –, de telles failles n'ont jamais donné lieu à exploitation effective. Comme pour la codification du monnayage, il est intéressant de noter que, à l'origine, Bitcoin « *contenait deux bogues totalement fatals qui rendaient le système entier sans valeur [,] heureusement, ils ont été découverts et corrigés avant qu['il] n'ait une valeur sérieuse* » : le premier, de type « *Theft* », permettait à « *n'importe qui [d'] écrire un scriptSig qui s'évaluait toujours à true et [ainsi, de] réclamer les pièces de n'importe qui d'autre [, et fut] corrigé dans la v0.3.2* » (Hearn 2013 ; Apodaca 2015). Les autres cas recensés reposaient sur des pratiques

³⁸¹ À l'extrême, une attaque par DOS peut être utilisée pour réaliser une « attaque par éclipse » en direction d'un opérateur de nœuds* cible. Cela peut permettre à un attaquant de faire planter les pairs de sa cible afin de « *monopoliser l'ensemble des connexions entrantes et sortantes de la victime, isolant ainsi cette dernière du reste de ses pairs dans le réseau* » (Goldberg 2015). Ce type d'attaque, outre le fait qu'il perturbe le réseau ou qu'il permet de filtrer les informations entrantes et sortantes de la victime, ouvre aussi à des attaques plus complexes : « course aux blocs » ; « fractionnement de la puissance de minage », « minage égoïste » ou encore « double dépense sans confirmation* », voir (*Ibid.*; Saad et al. 2019).

³⁸² L'étude de l'épisode de juillet 2015 montre que « *cette attaque a eu un impact négatif sur les transactions non spam, augmentant les frais moyens de 51% (de 45 à 68 satoshis/octet) et le délai de traitement de 7 fois (de 0,33 à 2,67 heures). Cela a montré qu'un adversaire qui est prêt à dépenser des montants modestes en bitcoins (au moins 49 000 USD) peut avoir des effets sur le reste des utilisateurs du réseau.* » (Lopp 2021)

non conseillées (partage physique ou à distance³⁸³ d'un ordinateur entre plusieurs utilisateurs) et ces vulnérabilités ont été « *considérée[s] comme un risque faible* » (Dashjr 2019). Celles étiquetées « *Exposure* », comme les précédentes, sont peu communes (au nombre de 4 ; crises n° 6, 16, 18 et 30) et n'ont pas donné lieu à exploitation. Elles renvoient à la possibilité pour un « *attaquant* » d'accéder à des données utilisateurs « *sensibles* » (clef privée stockée en clair³⁸⁴) et remettent en cause les propriétés attendues de la sécurisation de ses avoirs numériques. Les « *Fake conf* » (au nombre de 6 ; crises n° 9, 20, 28, 29, 32 et 33) correspondent aux situations où un « *attaquant* » peut potentiellement réaliser, en direction d'un acteur cible, une double dépense avec une confirmation seulement³⁸⁵. Bien que difficilement réalisables, des exploitations effectives ont été constatées³⁸⁶. Si l'expérience utilisateur est dégradée, particulièrement pour le receveur floué, le protocole n'est pas en cause. La convention du nombre de confirmations attendues pour considérer le paiement finalisé l'est. Les vulnérabilités étiquetées « *Deception* » voient un « *attaquant* » avoir le pouvoir de propager des informations erronées au sein du réseau* - une seulement a été décomptée, la crise n° 38 et ses conséquences potentielles étaient peu critiques : cette vulnérabilité permettait d'injecter à distance des données arbitraires dans le journal de débogage de la cible³⁸⁷. Enfin, le label « *Unknown* » est une catégorie valise où sont regroupées des vulnérabilités dont l'*« étendue des abus possibles est inconnue »*³⁸⁸ (nous en avons décompté 5 ; les crises n° 8, 25, 31, 37 et 38). Au sein de cette catégorie, l'évaluation de la gravité et des conditions effectives d'exploitation nécessite de s'intéresser à chacune des vulnérabilités concernées³⁸⁹, soulignant l'existence d'incertitudes et de risques émergents comme d'une normalisation encore partielle³⁹⁰.

Ce qui précède montre que le concept de crise est une « *catégorie indigène autant qu'un concept analytique* » : les matériaux disponibles pléthoriques, sur la crise Bitcoin CVE 2018 et les

³⁸³ Voir respectivement, <https://medium.com/@lukedashjr/cve-2018-20587-advisory-and-full-disclosure-a3105551e78b> pour la crise n° 36 ; https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2010-5141 pour la crise n° 1 ; et <https://github.com/bitcoin/bitcoin/issues/2838> pour la crises n° 22 [consultation au 08/11/2021].

³⁸⁴ Voir <https://bitcointalk.org/index.php?topic=51604.0> pour la crise n° 6, ou <https://github.com/bitcoinknots/bitcoin/blob/v0.13.1.knots20161027/doc/release-notes.md> pour la crise n° 30 [consultation au 03/11/2021].

³⁸⁵ Andresen explique cette attaque dans l'exposé des motifs du BIP 0016 relatif à la crise n° 9 : « *L'attaquant crée une transaction pay-to-script-hash qui est valide selon l'ancien logiciel, mais invalide pour la nouvelle implémentation, et s'envoie quelques pièces en l'utilisant. L'attaquant crée également une transaction standard qui dépense la transaction pay-to-script, et paie la victime qui utilise l'ancien logiciel. L'attaquant mine un bloc qui contient les deux transactions. Si la victime accepte le paiement à confirmation* unique, l'attaquant gagne, car les deux transactions seront invalidées lorsque le reste du réseau écrasera le bloc invalide de l'attaquant. L'attaque est coûteuse, car elle nécessite que l'attaquant crée un bloc dont il sait qu'il sera invalidé par le reste du réseau.* » (voir https://en.bitcoin.it/wiki/BIP_0016 [consultation au 03/11/2021]).

³⁸⁶ Comme l'explique Andresen dans le BIP 0050, « *pendant ce temps, il y a eu au moins une grande double dépense* » réussie de près de 10 000€ de l'époque, ciblant la bourse d'échange OKPAY, voir <https://bitcointalk.org/index.php?topic=152348.0> [consultation au 15/11/2021].

³⁸⁷ Voir <https://nvd.nist.gov/vuln/detail/CVE-2018-20586> [consultation au 15/11/2021].

³⁸⁸ Voir https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures [consultation au 15/11/2021].

³⁸⁹ Lors de la crise n° 8, Matt Corallo a trouvé un bogue rare et « *difficile à reproduire concernant le plantage de Bitcoin-QT* », qui laisse beaucoup d'interrogations : « *Est-il exploitable ? Un attaquant pourrait-il créer des messages de protocole bitcoin qui déclenchaient le bogue et compromettaient les ordinateurs Windows ? A-t-il déjà été exploité ?* » Les « Core Devs » d'avouer : « *Nous n'en savons rien* », même si « *nous pensons qu'il serait extrêmement difficile de créer un exploit utilisable* » (voir <https://gavintech.blogspot.com/2012/03/full-disclosure-bitcoin-qt-on-windows.html> [consultation au 15/11/2021]).

³⁹⁰ Ce qui transparaît dans ce mail : « *Quelqu'un garde-t-il une trace des bogues et des correctifs liés à la sécurité, [...] dans l'affirmative, cette liste peut-elle être partagée [...] ?* » Car « *aucun nouveau CVE n'a été publié depuis près de trois ans, [et] aucune information ne semble avoir été rendue publique. [...] Il serait très avantageux pour les utilisateurs finaux que la communauté des clients et des altcoins* dérivés de Bitcoin Core puisse être protégée contre les risques de fraude.* » (Liu 2017)

autres, permettent d’interroger les conditions présidant à ce que des événements soit *fabriqués comme crises et gouvernés* comme tels (Aguiton, Cabane et Cornilleau 2019, p. 11-12). Nous allons l’ expliciter par la suite.

III.2 DES MARQUES D’UNE POLITIQUE DE CRISES : UNE GOUVERNANCE DE HUIS CLOS ROUTINIÈRE

Bitcoin est vendu par certains comme un objet autonome et autorégulatoire, arguant du fait que ses codes protocolaires contiennent l’ensemble des règles et incitations nécessaires à son fonctionnement pérenne et soutenable. Pourtant, les codes Bitcoin, constituant sa gouvernance *par le protocole*, sont faillibles et dès qu’ils sont reconnus comme ne correspondant pas aux attentes de la communauté des usagers, ils entrent en crise. Dans cette situation où la gouvernance *par le protocole* est mise en défaut, il ne faut pas attendre d’elle qu’elle se remette en ordre. Cette situation nécessite une gouvernance *sur le protocole*, renvoyant à des activités humaines, médiatisées des dispositifs socio-techniques en dehors de la chaîne* : la gouvernance du répertoire logiciel Bitcoin Core qui, si elle n’épuise pas la gouvernance *sur l’infrastructure* de Bitcoin, y tient une place centrale. L’administration des codes s’inscrit pour bonne part dans des pratiques anciennes, initiées pour le développement des logiciels libres/ouverts, et suppose un enchevêtrement de relations interpersonnelles plus ou moins formelles, entre des volontaires souvent bénévoles (De Filippi et Loveluck 2016, p. 9). Ce constat d’humidité de codes moins « secs » contredit l’antienne de l’immutabilité de Bitcoin des *coiners**. L’histoire des crises montre que les codes sont modifiés continuellement, de manière incrémentale, mais aussi radicale. Cela soulève des questions. Qui, comment et pourquoi des acteurs non humains sont pointés comme défaillants ? Que recouvrent matériellement les codes protocolaires de Bitcoin ? Où, comment et par qui ce code peut-il être modifié ?

Chercher la matérialité des codes, c’est découvrir leurs dispositifs de production et de maintenance collaborative, et les acteurs qui en ont la charge. Dans notre cas d’étude et en l’absence d’activation de la faille, c’est la gouvernance *sur le protocole* qui fut prépondérante et qu’il nous faut éclairer. Ce terrain offre l’occasion d’aller au-delà des analyses réductrices, insistant sur les seuls acteurs non humains présents *on chain** – les noeuds* mineurs et complets – et leurs relations protocolaires automatiques et mécaniques. Il permet d’opérer un décentrement vers la dimension *off chain* et de mettre en exergue les acteurs, institutions, normes et conventions, les dispositifs et les arènes de débats prenant part activement à la résolution de cette crise, comme plus généralement à la maintenance et à l’évolution des codes sources Bitcoin. Il permet de décrire et d’analyser plus avant les statuts, rôles et fonctions de chacun, comme les modalités de leurs articulations pratiques : d’une part, comment les acteurs non humains sont autant des ressources mobilisées par les acteurs humains que des contraintes pesant sur leurs actions ; d’autre part, comment les interactions entre acteurs humains dépendent, pour bonne part et en plus de leurs fonctions relatives au sein du protocole, de leur insertion dans des réseaux* sociaux qui leur sont propres. La présentation que nous avons faite du bogue Bitcoin CVE 2018 et de sa résolution a fait apparaître une grande hétérogénéité d’acteurs non humains, « *on chain** » (les implémentations et versions logicielles variées structurant réseaux* et protocole), mais aussi et surtout « *off chain** », avec une grande multiplicité de dispositifs socio-techniques mobilisés. Nous avons aussi montré que des acteurs humains, peu nombreux et au statut particulier, ont pris part tant à la mise en crise qu’à la remise en ordre. Ce point souligne l’existence de sous-groupes (comme les développeurs*) structurant la communauté et de modalités d’interrelations particulières.

Il existe donc bien une gouvernance pour Bitcoin. L'analyse systématique des crises en offre une image incarnée, à rebours des analyses réifiantes que nous critiquons. Comme protocole, Bitcoin est régulé idéellement et matériellement : un cadre normatif l'enserre, composé des attendus des *bitcoiners** et dessinant l'*« état du monde considéré comme "normal" à partir [duquel] "est construit et alimenté»* un autre état du monde considéré comme critique (Aguiton, Cabane et Cornilleau 2019, p. 11). Concrètement, ces normalisations supposent que Bitcoin porte au sein de sa communauté un/des groupe(s) de normalisateur(s), dont l'activité repose sur des outils et dispositifs de diagnostic, de contention et de remédiation. Cette fabrique des crises et de leur gouvernance, faite d'interactions hétérogènes reposant sur un ensemble composite d'espaces, d'interlocuteurs, de dispositifs techniques, nous allons l'expliciter.

III.2.1 Des acteurs au cœur de la gouvernance sur le protocole

Si un acteur non humain aussi essentiel qu'un client Bitcoin et ses codes fait défaut et entre en crise, c'est la gouvernance *par* le protocole qui est remise en cause. L'état de crise révèle ce que les acteurs considèrent comme « *normal* » et ce qui ne l'est pas (Aguiton, Cabane et Cornilleau 2019) : est reconnu, plus ou moins brutalement, un hiatus entre les actions prescrites par la conception (et les concepteurs) et les actions effectivement réalisées (Akrich, 2010). Ce hiatus interroge les dichotomies opposant la routine au dysfonctionnement, le bogue à l'attaque, le normal à l'exceptionnel, comme il éclaire les acteurs et dispositifs participant de leur établissement.

De l'âme des acteurs non humains : d'un « esprit du code » excédant sa « lettre »

Au titre de l'interrogation précédente, l'acception rigoriste du slogan « *code is law* » vide de tout fondement les concepts mêmes de failles, de vulnérabilités, de bogues, voire d'attaques. Du point de vue qui voudrait que la gouvernance d'une CM doit relever d'une « loi de Szabo » où le code informatique est souverain (Zamfir 2019, cf. Chap. II section II.3.3), la « déférence au code » (Hinkes 2021) et à l'*« autorité algorithmique »* (Lustig et Nardi 2015) est totale et sans limites : tous les résultats d'un code sont par définition normaux, indiscutables et légitimes. Cela signifie-t-il que près de 83% des nœuds* vulnérables (Tableau 3 ci-dessus) et leurs utilisateurs avaient « *fondamentalement opté pour les règles de consensus de Bitcoin telles qu'elles existent* » [Corallo, Entretien n° 15] dans leurs codes de versions ? D'après Awemany (2018), critiquant au passage la centralité de Bitcoin Core, avec le Bogue Bitcoin CVE 2018 « *certaines choses ont complètement disparu [...] par exemple l'idée de Core selon laquelle "le code est la loi". Si le code est la loi, cela signifie-t-il que vous devez accepter l'inflation maintenant ? Ou est-ce en fait les développeurs* de Core qui dirigent le navire ?* ». Non, la remise en cause du consensus sur la validité des transactions* et le monnayage induit par ces codes n'est ni volontaire, ni souhaitée, seulement le résultat de l'incertitude radicale et de la rationalité limitée des acteurs inhérente à leurs activités. D'où le paradoxe. De nombreux *coiners** se revendiquent du camp de la règle radicalisée, notamment Satoshi : ce qui est écrit dans le code est/doit être indiscutable et immuable. Pourtant, les mêmes mobilisent une terminologie de crise – parlant de faille, d'attaque, de l'*« honnêteté »* attendue des nœuds* (Nakamoto 2008) par exemple - qui ajoute à ces codes un supplément d'âme, une normativité sans laquelle ils n'ont sens. À la question de savoir pourquoi Song qualifie de « *pathologiques* » les transactions* incriminées dans la faille CVE 2018 et s'il faut considérer le changement des versions vulnérables comme une mise à niveau des règles de consensus (cf. un *Fork**, cf. section III.3 suivante), Song de nous répondre : « *Hum, Code, Code, donc ça dépend, c'est une version multiple du code, et ça a affecté une gamme particulière de versions [qui] allait à l'encontre de ce qui était là avant donc, ils... ce ne serait pas... un Fork... c'est vraiment une correction d'un code qui est sorti du consensus... si ça a un sens [...] et le code est la loi dans le sens où, ce n'est pas seulement le code maintenant. C'est tout le code d'avant et pour le code d'avant* »

cette transaction pathologique aurait été rejetée [...], ce n'est pas nécessairement que nous avons brisé le principe du "Code is Law" » [J. Song, Entretien n° 17]. Cela a un sens : ces codes et ses attendus d'« avant », bien que minoritaires dans la structuration du réseau*, devaient primer sur le cadre formel devenu majoritaire.*

S'il faut prendre au sérieux le slogan « Code is Law », c'est dans le sens originel qu'il revêt chez Lessig (2000), et qu'aurait « *un petit peu mal interprété* » beaucoup de *bitcoiners** [L. Thiébault, Entretien n° 21, rejoint par Roussel, Entretien n°11]. À revenir au texte de Lessig (2000), l'un des juristes en première ligne de la contre-offensive contre « *la privatisation croissante du patrimoine intellectuel et culturel de l'humanité* » (avec J.Litman, Y.Benkler, L.Lessig, J.Boyle ; Coriat et Broca 2015, p. 273, cf. Chap. I, section I.1.1), il semble que les *coiners** lui donnent un sens opposé. Sa formule « Code is Law » mettait en garde contre l'idée que le *gouvernement* est le seul danger pour les libertés. Contrairement à l'interprétation qui prévaut chez les *coiners**, Lessig affirmait que la technique dissimule des « *régulations* », que le cyberspace a « *son propre régulateur* » et qu'ils sont tout aussi menaçants : « *le code[,] le logiciel et le matériel qui font du cyberspace ce qu'il est* » définissent qui peut avoir « *un impact sur qui* », « *voire quoi, ou sur ce qui est surveillé* » et, plus généralement, « *la manière dont nous vivons le cyberspace* » (Lessig 2000). Code et développeurs*, architecture et architectes, s'imposaient comme un cadre para-légal produit par de nouveaux législateurs. Ce slogan impose une mise en parallèle du code et de la loi, non l'hypothétique substitution de l'une, défaillante et arbitraire car « *humide* », par de la technique efficace et neutre car codée « *en sec* », substitution que suppose N. Szabo (2008b). Quoiqu'en dise cette figure de l'interprétation rigoriste du « *Code is Law* », si le droit est conflictuel du fait de sa dimension interprétative, il en est de même pour le « *code informatique et [les] fichiers lisibles par ordinateur (dans la mesure où : [si en temps normal] un ordinateur les traite de manière cohérente)* » (Szabo 2008b), en temps de crise justement, il les traite de manière non cohérente . Sa distinction entre les normes légales et réglementaires, considérées comme du « *code humide* » « *interprété par le cerveau* » et celles informatiques, relevant de « *code sec* » interprété « *par les ordinateurs* » ne tient pas. La dimension interprétative inhérente au droit l'est aussi pour les codes : la distinction clef en philosophie du droit, opposant les concepts de « *lettre de la loi* » à celui de « *son esprit* », reste utile. L'application d'une loi suppose une activité interprétative du juge, mêlant la lettre de la loi (les textes législatifs et l'interprétation littérale qu'ils permettent) et l'esprit de la loi, censé saisir les intentions sous-jacentes d'un texte législatif. Lorsque les textes sont flous ou mal taillés pour couvrir explicitement certaines situations, l'esprit de la loi peut être mobilisé afin de combler ce vide juridique formel. De même, les règles protocolaires canoniques de Bitcoin vont au-delà de leur syntaxe et de leur sémantique (la lettre des codes), englobant les intentions des développeurs*, les débats communautaires et leurs compromis, qui se traduiront dans l'inclusion/exclusion de nouvelles fonctionnalités, la publication de nouvelle version, voire de *Fork**. Les promoteurs de la « *loi de Szabo* » confondent le légal et le légitiment, suivant une acceptation rabattant l'esprit du code sur sa seule lettre : aucun dysfonctionnement, seulement des fonctionnements. Néanmoins, ces représentations idéales (et stéréotypiques) n'épuisent pas l'éventail des vues présentes dans la communauté sur ce qu'est une bonne gouvernance de CM. Dans le sens de la conception idéal-typique opposée (cf. la « *loi crypto* » ou « *crypto law* » de Zamfir concernant la gouvernance d'une CM 2019, Chap. II section II.3.3), des *coiners** accordent une importance centrale à la lettre du code, dont ils soulignent en creux les processus qui en supportent mise en forme et expression. Pour A. Roussel (juriste lui aussi), l'esprit du code prime : [Nous] « *Tu viens du milieu juridique, tu distingues la lettre de la loi de l'esprit de la loi ?* » [Lui] « *Oui, voilà exactement. Et beaucoup de gens qui ont la position très stricte dans "Code is law", ils n'ont pas cette notion [,] le code a quand même été fait par des gens, et [...] le contrat social qui se cristallise dans le code peut évoluer avec le temps [induisant] un décrochage entre le code et le contrat social,*

ce qui fait qu'à un moment donné [...] on abolit le code [,] le contrat social [est] plus fort que le code, de toute façon. » (Entretien n° 11).

Paradoxalement, les *coiners** les plus rigoristes, qui rejettent l'idée qu'une CM dispose d'une gouvernance autre que ses codes, par le jargon et les catégories qu'ils mobilisent, peuvent en mettre en cause la légitimité de certains résultats. Tout en l'invisibilisant, ils mobilisent eux aussi une normativité supposant un « contrat social » et des dispositifs variés, sans lesquels aucun décalage problématique entre le produit désiré d'un code (son « esprit ») et le résultat de sa « lettre » ne peut être reconnu. Ce hiatus et sa reconnaissance renvoient à un processus de normalisation à partir duquel les *coiners** dessinent différents types de crises/modifications de règles protocolaires consensuelles canoniques.

Quatre situations apparaissent possibles, suivant que coïncident ou non « les codes » logiciels protocolaires (« leur lettre ») et les attentes qu'en ont les membres de la communauté (leur « esprit »), comme représenté dans le Tableau 5 suivant.

Tableau 5 : Les deux grandes familles de crises protocolaires

	...ce qui est attendu = considéré comme légitime par le consensus social	...ce qui n'est pas attendu = considéré comme illégitime par le consensus social
Le code permet ...	<p style="text-align: center;">[a] Situation normale</p> <p><u>Action : <i>Statu quo</i></u></p> <p><i>Ex. : contrôle de la double dépense, création monétaire qui suit l'échéancier prévu, etc.</i></p>	<p style="text-align: center;">[b] Crise « de vulnérabilité »</p> <p><u>Action : Correction d'un bogue (lettre du code) pour retrouver le caractère exécutoire des normes passées, toujours légitimes (esprit du code)</u></p> <p><i>Ex. : double dépense et régulation de la création monétaire suivant les règles et l'échéancier prévu (Cas CVE 20182).</i></p>
Le code ne permet pas...	<p style="text-align: center;">[c] Crise « d'évolution »</p> <p><u>Action : Application de nouvelles règles protocolaires (lettre du code) pour sortir des normes passées, devenues illégitimes et s'adapter à l'évolution des attentes communautaires (esprit du code)</u></p> <p><i>Ex. : SegWit et le Scaling Debate; The DAO hack.</i></p>	<p style="text-align: center;">[d] Situation normale</p> <p><u>Action : <i>Statu quo</i></u></p> <p><i>Ex. : rejet des doubles dépenses, invalidation de toute création monétaire qui ne suit pas les règles et l'échéancier prévu, etc.</i></p>

Source : Rolland Maël

Deux situations normales, en bleu, se dégagent : le cas [a] se caractérise par le fait que le code permet/produit des résultats considérés comme légitimes par le consensus social en vigueur dans la communauté de paiement (pouvoir réaliser/recevoir une transaction* en temps voulu, par exemple). Le cas [d], à l'inverse, voit les codes interdire les actions et résultats considérés comme illégitimes du même point de vue (empêcher la réalisation d'une double dépense, par exemple). En contrepartie de cette normalité apparaissent deux cas « anormaux », où lettre et esprit des codes ne coïncident pas. Le cas [b] correspond à une situation caractérisée par le fait que les codes permettent des actions/résultats considérés comme manifestement illégitimes à consensus social inchangé (permettre la réalisation d'une double dépense, par exemple). La mise en crise, l'étape de déclenchement qui renvoie à la prise de conscience de l'existence d'une vulnérabilité, est brutale et située (que ce soit par exploitation publique ou par divulgation responsable privée). Nous la qualifions pour cela de « crise de vulnérabilités ». À l'inverse, le cas [c] renvoie à des situations plus latentes, où la lettre du code perd en légitimité chez certains, ce qui les conduit à vouloir l'amender : la légitimité des codes est remise en cause en ce qu'ils ne permettent pas – en l'état – des actions/résultats pourtant souhaités par les membres de la communauté. Cette crise est qualifiée de « crise d'évolution », la reconnaissance d'une transgression de la lettre des codes à leur esprit n'a rien d'évident et, contrairement au cas précédent, la mise en crise peut prendre du temps, voire ne jamais advenir. Cela passe par l'ouverture de négociations communautaires, supposant la construction préalable d'un problème public, par des acteurs et groupes plus ou moins minoritaires,

inaudibles et/ou invisibilisés. Ces acteurs devront convaincre les autres franges communautaires du bien-fondé de leurs modifications (cf. « Scaling Debate », Chap II. Section II.3.3).

Il existe différents types de crises dont nous construisons deux familles génériques : les « crises de vulnérabilité » et les « crises d'évolution ». Elles renvoient à un travail de normalisation, permettant de standardiser et classifier, au-delà des crises, les différents types de modifications de codes protocolaires et leur forme attendue. Ce travail suppose l'existence de lieux, cadres et dispositifs dédiés à la fabrication de ces codes, et, finalement, l'existence d'une chaîne de montage, articulant des ouvriers plus ou moins spécialisés. Intéressons-nous d'abord à l'objet de cette normalisation des crises, ces implémentations et versions de clients Bitcoin jugés défaillants.

La diversité des acteurs non humains en question : l'hégémonie de « Bitcoin Core » en crise ?

Que la faille CVE 2018 soit multiforme, impliquant deux types de bogues selon les implémentations et les versions des clients Bitcoin concernées, illustre la dimension infrastructurelle et écosystémique de Bitcoin. En tant que protocole, Bitcoin (et toute CM) doit pouvoir être implanté suivant différents codes logiciels. Qu'il soit structuré matériellement par des logiciels hétérogènes (différences d'architecture, de langage de programmation*, d'options), tant que ses clients sont compatibles entre eux et respectent les règles canoniques consensuelles, le réseau* sera unitaire et cohérent. Dans le champ des CM et de leur protocole de registre* distribué, deux types d'« *implémentations concurrentes* » sont à distinguer : les implémentations incrémentales simples qui « *ne modifient pas les règles de consensus et ne réimplémentent pas la base de code* » et les « *implémentations indépendantes* » qui, radicalement différencieront, sont « *réimplémentées sans utiliser le code de Bitcoin Core* », par exemple avec « *un nouveau langage de codage [...] afin d'essayer d'exploiter [c]es avantages* » (Bitmex Research 2018).

La crise que nous avons choisi d'étudier dévoile le travail de maintenance, quotidien et de longue haleine, qu'impose Bitcoin à certains membres de sa communauté, et pointe la centralité de « Bitcoin Core ». Les implémentations indépendantes ont toujours été très minoritaires dans la structuration du réseau* et la majorité n'est que de type incrémental : peu différencieront, ces implémentations reposent sur « Bitcoin Core » qui tient lieu de « spécification protocolaire »³⁹¹. Cette présence de l'implémentation Bitcoin Core s'explique par les choix et développements historiques qui, par un effet de sentier, ont conduit à privilégier une implémentation logicielle unique. Dès l'origine, Bitcoin se présente comme un logiciel dont les codes sources sont ouverts (sous licence MIT, cf. Chapitre I). Par ce choix, Nakamoto rend les codes sources du logiciel Bitcoin qu'il publie facilement auditables, copiables, modifiables, ouvrant à la production d'autres clients par d'autres équipes d'acteurs. Mais Nakamoto ne publia jamais à proprement parler de cahier des charges (« *specs* ») explicitant précisément son protocole. Il est peu probable de voir émerger un tel cahier des charges « *car personne n'a l'autorité pour en écrire* » (Lopp 2018) : « *les specs, c'est le code de Bitcoin Core, enfin, de manière implicite finalement. Parce que même pas le "White Paper" ben, il n'y a pas de "specs" du tout, il n'y a rien, il n'y a pas de détails. Du coup, c'est la première implémentation et les changements qui ont été faits après [...]* » qui tiennent ce rôle [A. Le Calvez, Entretien n°20]. La première implémentation du logiciel Bitcoin (Bitcoin v0.1) de

³⁹¹ « Bitcoin Knot », par exemple, développé dès décembre 2011 sous le nom de Bitcoin Next-Test par Luke jr, fut concernée par la faille CVE 2018. Cette implémentation dérive directement de la branche « master » de Bitcoin Core et implémente en avant-première les fonctionnalités qui y sont proposées à la fusion.

Nakamoto fut publiée sur la forge logicielle* « sourceforge », le 8 janvier 2009 (Nakamoto 2009³⁹²). Elle prenait la forme d'un fichier « .rar », sans gestion de contrôle des sources, et les développeurs* souhaitant échanger des correctifs avec Nakamoto devaient le faire par mail³⁹³ (Lopp 2018). « Sirius-m »³⁹⁴, le second développeur* Bitcoin après Nakamoto (bit2me Academy) créa le 30 octobre 2009 la première version du répertoire logiciel (ou « repo ») sur « sourceforge »³⁹⁵ (*Ibid.*). Le logiciel de Nakamoto allait servir de base au développement de deux implémentations : « bitcoind »³⁹⁶ et « BitcoinQt », qui seront fusionnées et renommées BitcoinQT à partir de la version 0.5.0, publiée fin 2011³⁹⁷. Dès lors, BitcoinQt tint lieu d'implémentation référente et, la même année, la gestion du projet fut migrée de la plateforme « sourceforge » à « Github » (Lopp 2018). Finalement, en 2014, elle est renommée Bitcoin Core (*Ibid.*) au prix d'une controverse³⁹⁸.

En effet, la position de monopole de Bitcoin Core et le statut subordonné des autres implémentations ne s'expliquent pas seulement par cette absence de spécifications. Elle est délibérée et organisée dès l'origine, l'unicité des règles et la stabilité du protocole en dépendraient : « *la nature du bitcoin est telle qu'une fois la version 0.1 publiée, la conception de base était gravée dans la pierre pour le reste de sa vie. [...] Je ne pense pas qu'une seconde implémentation compatible de Bitcoin soit une bonne idée. Une si grande partie de la conception dépend de l'obtention par tous les nœuds* de résultats exactement identiques et synchronisés qu'une seconde implémentation serait une menace pour le réseau** ». » (Nakamoto 2010e)³⁹⁹ De plus, cela doit faciliter la maintenance car la « *version officielle* » implique déjà une charge de travail importante, en particulier suivant les contraintes de rétrocompatibilité que Nakamoto s'impose⁴⁰⁰. Dès cette origine, Bitcoin Core s'est donc imposé comme « *le point central de développement* ». Accumulant tous les talents et le travail accompli, son code serait « *le plus performant, le plus robuste et le plus sûr* », d'où le fait que les opérateurs de nœuds* l'utilisent lui : « *il est un peu plus sûr [...] car vous avez plus de chances d'être compatible, bogue pour bogue, avec la majeure partie du reste du réseau** » (*Ibid.*, comme confirmé par JF. Augusti, Entretien n° 18). Ainsi, l'existence d'implémentation incrémentale, comme « *forme de concurrence, qui ne modifie pas délibérément les règles de consensus et ne réimplémente pas le code, n'est pas du tout controversée* » (BitMEX 2018), contrairement aux implémentations indépendantes, un « *sujet très controversé et qui divise* » (Bitmex Research 2018) de longue date : visible lors du « Scaling Debate » (cf. Chap II section

³⁹² Voir le mail original ici : <https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html> [consultation au 11/10/2021].

³⁹³ Les échanges entre Nakamoto et Finney sont consultables ici : <https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf> (Consultation au 11/10/2021)

³⁹⁴ Marty Malmi de son vrai nom, que l'on a déjà rencontré dans le chapitre II pour le premier achat en BTC dans le monde réel avec la désormais fameuse Pizza (bit2me Academy).

³⁹⁵ <https://sourceforge.net/p/bitcoin/code/1/> [consultation au 11/10/2021].

³⁹⁶ Bitcoind est une implémentation logicielle qui met en œuvre le protocole Bitcoin pour l'utilisation de l'appel de procédure à distance (RPC). Elle correspond historiquement à la deuxième implémentation du client Bitcoin. Voir <https://en.bitcoin.it/wiki/Bitcoind> [consultation au 11/10/2021].

³⁹⁷ <https://bitcoin.org/en/release/v0.5.0> [consultation au 11/10/2021].

³⁹⁸ <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 11/10/2021].

³⁹⁹ Discussion originale : <https://bitcointalk.org/index.php?topic=195.msg1611#msg1611> [consultation au 12/10/2021].

⁴⁰⁰ Dans cet échange, il déclare : « *une deuxième version serait un énorme problème de développement et de maintenance pour moi. Il est déjà assez difficile de maintenir la compatibilité ascendante tout en mettant à niveau le réseau sans qu'une deuxième version ne vienne verrouiller les choses. Si la deuxième version se plantait, l'expérience de l'utilisateur se répercuterait négativement sur les deux, même si cela renforcerait au moins auprès des utilisateurs l'importance de rester avec la version officielle. Si quelqu'un se préparait à intégrer une seconde version, je devrais diffuser beaucoup d'avertissements sur les risques liés à l'utilisation d'une version minoritaire. C'est une conception où la version majoritaire l'emporte en cas de désaccord, et ça peut être assez moche pour la version minoritaire. Je préfère ne pas m'y attarder, et je n'ai pas à le faire tant qu'il n'y a qu'une seule version* » ; <https://bitcointalk.org/index.php?topic=195.msg1617#msg1617> [consultation au 12/10/2021].

II.3.3), cette division était apparue dès 2014, dans la controverse entourant le changement de nom en « Bitcoin Core »⁴⁰¹. L'objectif du changement de nom était de « *supprimer la confusion entre le réseau* Bitcoin et l'implémentation du client de référence que nous maintenons dans ce dépôt, tous deux nommés confusément "bitcoin"* » (Van der Laan)⁴⁰². Mais certains développeurs* reconnus (P. Todd, Luke Jr et G. Maxwell⁴⁰³) voyaient dans le qualificatif « Core » une dénomination vectrice d'une centralisation symbolique trompeuse⁴⁰⁴. Le problème était que cela « *implique que vous en ayez besoin....* » (Todd)⁴⁰⁵, laissant croire qu'elle est nécessaire à l'utilisation de Bitcoin, les autres clients étant « *traité[s] comme une sorte de client de "seconde classe"* » (Luke JR⁴⁰⁶) : ce « *terme "core" devrait être utilisé pour la partie critique du consensus, et non pour tout le code supplémentaire de portefeuille, de relais, etc. que l'implémentation de référence ajoute* » (Todd⁴⁰⁷). La critique de la domination exercée par Bitcoin Core sur le réseau* n'est pas que sémantique. Contre Nakamoto et ses suiveurs, certains développeurs* estiment que cette exclusivité représente une menace pour la sécurité de Bitcoin. C. Jeffrey, développeur* de l'implémentation indépendante « Bcoin »⁴⁰⁸, fit polémique en 2017. Cherchant à alerter sur le risque systémique posé par ce qu'il considère comme une monopolisation du développement de Bitcoin, il révéla publiquement une faille de Bitcoin Core non encore patchée⁴⁰⁹ (Jeffrey 2017; Apodaca 2017 ; Entretien n°21 ; Observation participante n° 15 Bitcoin 2017, Annexe n°III.2 et III.4). Comme la crise Bitcoin CVE 2018 l'illustre parfaitement, l'hétérogénéité des versions logicielles au sein de « Bitcoin Core » implique que « *chaque révision de Bitcoin Core introduit le risque d'un bug de consensus de rupture de chaîne, [soit] exactement la [situation] que les implémentations de noeuds* alternatifs sont accusées de promouvoir* » (Apodaca 2017). Sans réellement gagner en sécurité du côté compatibilité, cela réduira la résilience du réseau*. Les besoins de sécurité et décentralisation de Bitcoin commanderaient à ce qu'il soit fondé sur plusieurs implémentations indépendantes assurant que des implémentations continuent à fonctionner indépendamment des failles rencontrées par une implémentation particulière. Cela conduit certains à déceler dans ce monopole Bitcoin Core l'existence d'« *une structure de pouvoir invisible qui prive de ressources les équipes extérieures à cette structure* », avec « *une mafia qui squatte le core dev et empêche les autres équipes de développement de concourir* », selon les mots extrêmes d'A. Taaki⁴¹⁰.

⁴⁰¹ Voir les discussions : <https://github.com/bitcoin/bitcoin/pull/3408> ; <https://github.com/bitcoin/bitcoin/issues/3203> ; <https://github.com/bitcoin/bitcoin/pull/3400> [consultation au 11/10/2021].

⁴⁰² <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 11/10/2021].

⁴⁰³ N'ayant pas « *d'avis tranché* », la proposition obtiendra son « accord » (<https://github.com/bitcoin/bitcoin/issues/3203#issuecomment-28133803>) [consultation au 12/10/2021].

⁴⁰⁴ https://en.bitcoin.it/wiki/Bitcoin_Core#Naming_Controversy [consultation au 12/10/2021].

⁴⁰⁵ https://www.reddit.com/r/Bitcoin/comments/60jqm2/a_proposal_for_and_demo_of_a_new_bitcoin_address/df73k2h/ [consultation au 12/10/2021].

⁴⁰⁶ <https://github.com/bitcoin/bitcoin/issues/3203#issuecomment-27787010> [consultation au 12/10/2021].

⁴⁰⁷ <https://github.com/bitcoin/bitcoin/pull/3408> [consultation au 12/10/2021].

⁴⁰⁸ Bcoin est une implémentation indépendante de Bitcoin écrite en JavaScript, publiée en 2014 par Fedor Indutny. Portefeuille léger de navigateur, son développement a été réalisé ensuite par Jeffrey, pour Purse.io.(Apodaca 2017; Chiang 2017).

⁴⁰⁹ La présentation de Chris Jeffrey démontrait ce point via une faille DOS. Cette divulgation a engendré des débats et critiques, parfois véhémentes, son caractère « responsable » et « légitime » est contesté, puisque la présentation n'a pas attendu le patch alors que les organisateurs de l'événement avaient demandé de ne pas la faire pour cette raison [L. Thiébaut, Entretien n° 21]. Lui argue que l'équipe Core a été informée plusieurs mois en avance et n'a pas réagi, justifiant des problèmes de disponibilité* qui vont dans le sens de ce que sa démonstration visait à démontrer (<https://diyhpl.us/wiki/transcripts/breaking-bitcoin/2017/2017-09-10-christopher-jeffrey-consensus-pitfalls/>) [consultation au 12/10/2021].

⁴¹⁰ <https://twitter.com/Narodism/status/1445335283533242370> [consultation au 12/10/2021].

Il est temps de présenter les acteurs humains ayant à leur charge maintenance et sécurité de Bitcoin, qui sont apparus dans l'histoire du bogue analysé.

Qui peut modifier Bitcoin ? Bitcoin Core, un groupe en charge de maintenir et sécuriser Bitcoin ?

Comme rappelé en introduction du chapitre, il n'est pas erroné de dire, comme certaines critiques, que la plupart des *bitcoiners** sont peu préoccupés des bogues qui pourraient toucher Bitcoin : les *bitcoiners** le concèdent, « *la menace des bogues logiciels est sévèrement sous-estimée dans le monde des cryptomonnaies**. » (Fields 2018). Mais ce n'est sûrement pas parce que les utilisateurs auraient « *une confiance aveugle* [...] *dans les codes et l'algorithme* » Ponsot (2021, p. 2) : leur *foi* est moins « *dans le bitcoin* » que dans les « *super codeurs* » qui en ont la charge (« *In Super Coders We Trust* »)⁴¹¹. Bitcoin est construit autour de préoccupations sécuritaires. À l'origine, Nakamoto avait même intégré à Bitcoin un système d'alerte visant à informer l'ensemble des nœuds* d'un problème éventuel, système rapidement supprimé, car il correspondait à « *un point de contrôle unique* » (Hertig 2018b). Nos analyses dévoilent une communauté Bitcoin fragmentée, selon une division sociale du travail distribuant confiance, délégations et comptes à rendre entre groupes composant sa communauté. La surprise qui a entouré le bogue CVE 2018 (Song 2018c) reflète en partie cette spécialisation, en mettant au jour des membres en charge d'administrer les codes et les crises qu'ils rencontrent. Cette surprise dénote en creux des attentes déçues : ils s'attendent à ce que des audits et « *relectures du code* [soient] *faites* » (*Bitcoin Q&A* 2018). L'anticipation et l'administration des crises, qu'elles soient « de vulnérabilité » ou « d'évolution », est déléguée à un groupe d'acteurs plus techniciens dont c'est « *définitivement une grande préoccupation* [...] *pendant les premières années où j'ai travaillé sur Bitcoin Core et sur le logiciel Bitcoin* [dès 2011, NdA], *notre plus grande préoccupation était* [la survenue d'] *un bogue et [...]* *que tout d'un coup, tout s'écroulait et qu'il n'y avait rien qui puisse être sauvé du système* » (McCormack et Corallo 2019).

Difficile de ne pas voir que le groupe des « Core Devs » dont fait partie Corallo, au centre des évènements restitués, tient effectivement le rôle d'« *autorité* [pouvant] *intervenir et sauver la situation* » (Varoufakis 2013) quand elle s'écarte des attendus communs. Ces membres volontaires disposent de capitaux culturels (savoir et savoir-faire) *ad hoc* hautement spécialisés. Ils ont la charge, plus ou moins formelle (comme avec les « Core mainteneurs », cf. section suivante), de maintenir et corriger le logiciel Bitcoin (Lopp 2018 ; Song 2019). L'optimisation des codes et la gestion des failles sont pour eux des activités quotidiennes. À la manière des pierres de l'église de Sainte-Anne étudiées par Edensor (2011, cité par Denis 2020)⁴¹², si, pour de nombreux *bitcoiners**, Bitcoin apparaît d'abord comme extrêmement « sécurisé », « stable » et « immutable », du point de vue des techniciens chargés de sa maintenance, il leur apparaît fragile et jamais stabilisé/ossifié : « *le logiciel chargé de faire respecter les règles de validation** *devra toujours évoluer. Des changements sont constamment apportés pour améliorer les performances, ajouter des fonctionnalités, renforcer la sécurité, etc.* » (Fields 2018). « *Bitcoin Core est très optimisé* » et il doit le rester : d'où une PR 9049 proposée et acceptée. Et ce travail quotidien implique que « *nous continuerons à voir des bogues. Tous les logiciels ont des bogues. Il n'existe pas de logiciel sans*

⁴¹¹ Voir le tweet original : <https://twitter.com/APompliano/status/1420095187578195974?s=20> [consultation au 14/10/2021].

⁴¹² Edensor (2011), étudiant la matérialité de la pierre de l'église Sainte-Anne, saisit comment cette entité, apparaissant « comme la chose la plus immuable qui soit », porte néanmoins « aux yeux et aux mains des ouvriers » qui la restaurent « des propriétés instables [...] », la pierre est sujette à de nombreuses détériorations (ex. décoloration, effritement, fissuration...) qui compromettent les « caractéristiques esthétiques de l'édifice patrimonial [et] sa pérennité même » (Denis 2020, p. 287).

bogue » (Antonopoulos 2018). Ce regard d'expert met en exergue la relativité de représentations et des attendus des *coiners*^{*413}.

Le « *plus grand défi de Bitcoin* » du groupe des « Core Devs » est d'« *éviter les bugs logiciels catastrophiques* » (Fields 2018). Si leurs pratiques empruntent au secteur de la production logicielle et de la sécurité informatique, ils sont conscients des enjeux spécifiques posés par les CM et leur protocole ouvert. Travailler sur Bitcoin s'apparenterait à de l'ingénierie à haut risque. Son logiciel « *est extrêmement complexe, en particulier le code au niveau du consensus [qui] est la forme la plus difficile de développement logiciel qui existe aujourd'hui [,] probablement proche de l'ingénierie aérospatiale, du fait que [...] chaque changement minuscule dans le code peut avoir des effets considérables.* » (Antonopoulos_2018). M. Corallo abonde, ajoutant que les pratiques de développement de Bitcoin gagneraient à s'inspirer de logiciels comme ceux « *de sécurité vitale, les appareils médicaux, les avions, ce genre de logiciels* » (McCormack et Corallo 2019). Il reste des contraintes spécifiques posées aux CM. Encore expérimental, leur caractère « *décentralisé* » ou tout du moins « *distribué* »⁴¹⁴ et le caractère hautement monétisable des failles font des CM « *un défi d'ingénierie unique* » (*Ibid.*) et « *un "Far West" virtuel* » exposant à « *un risque élevé de bogues* » (Böhme et al. 2020, p. 3) : une CM repose « *sur des systèmes distribués [et des] outils cryptographiques complexes, [...] issus de la recherche de pointe qui n'ont pas été largement évalués* » ; la concurrence « *féroce* » entre CM induit des mauvaises pratiques, pouvant pousser « *les développeurs* à sauter des étapes importantes nécessaires pour sécuriser leur base de code* » ; enfin, « *la forte prévalence des bogues est exacerbée par le fait qu'elles sont si facilement monétisables [...] les exploits qui volent des pièces sont à la fois lucratifs pour les cybercriminels et préjudiciables pour les utilisateurs et les autres parties prenantes.* » (Böhme et al. 2020, p. 3)

Corallo [Entretien n°15] et ses collègues de bureau font partie des développeurs*, peu nombreux, ayant réussi à se faire financer. À l'exception de l'entreprise de Corallo et ses collègues, « *ChainCode labs* », ou encore de « *Blockstream* », qui offrent des contrats de travail permettant de financer leurs travaux sur Bitcoin Core⁴¹⁵ (BitMEX Research 2020a), bien peu nombreux sont les

⁴¹³ Corallo, par exemple, partant du risque de bogue et de scission de chaîne, critique la convention entourant la finalité de paiement de Bitcoin fixée à 6 confirmations* (cf. section III.1.2 précédente), car elle ignore le temps nécessaire à cordonner une remise en ordre : « *effectuer des transactions à 3 confs, 6 confs, 12 confs est vraiment risqué [car] effectuer des transactions dans un délai inférieur au temps que les gens peuvent raisonnablement consacrer à répondre à un problème, à en identifier la cause et à le résoudre, ce qui n'est certainement pas deux heures. Vous introduisez beaucoup de risques.* » (Annexe IV.2, Observation participante n°25, retranscrit chez Osuntokun et al. 2019).

⁴¹⁴ Dans ce passage, Corallo revient sur le fait que, au sein de ces industries, la centralisation facilite les procédures de développement et de tests : « *leur solution est généralement de tout exécuter trois fois ; sur trois implémentations différentes et sur trois processeurs différents fonctionnant sur trois systèmes différents et vous choisissez juste celui qui est répété, d'accord. Donc vous avez les différents systèmes pour voter sur ce qu'est la solution.* » (McCormack et Corallo 2019)

⁴¹⁵ « *C'est tous des gens qui sont de leur côté, qui font des trucs, tu peux en avoir quelques-uns chez Blockstream mais c'est... et même, enfin je veux dire, Blockstream aujourd'hui je considère que c'est plus une boîte de recherche, tu vois* » [N. Bacca, Entretien n° 8]. Blockstream faisait partie des sponsors des évènements « *Breaking Bitcoin* » (Observation participante n° 14 et 25, Annexe n°IV.2), dont l'une des organisatrices nous apprend que « *Chaincode Lab* » organise aussi des formations « *sur plusieurs semaines de « "relecture" ("review") autour de la proposition de modification "Taproot" [...] organisée par des core devs. [...] Et en fait c'était sur 7 semaines normalement, c'était quatre fois par semaine, 40 heures par semaine. J'ai arrêté parce que c'était trop... trop chronophage, j'étais un petit peu larguée et en fait c'était une review avec toutes les semaines un sujet différent sur un petit peu de tout : "« Taproot", "», "« Grassroot", "», "« Schnorr", "», "« MAST" [...]. On était 160 au début, je crois que ça a terminé avec beaucoup moins [...]. J'étais déjà extrêmement contente que leurs initiatives au groupe 160 personnes, j'ai trouvé que c'était vraiment génial, ils ont organisé ça mais de manière incroyable, les mails, les machins... on sentait vraiment qu'il y avait un énorme investissement de la part des organisateurs pour faire en sorte de rendre le travail fluide pour tout le monde ».*

développeurs* Bitcoin à pouvoir en vivre [Stéphane Roche, Anon 1, 2 et 3 ; Entretien n° 23, 1, 2 et 3]. Le financement des personnes en charge de la maintenance et de la sécurité de la couche protocolaire de Bitcoin est « *un problème [...] intéressant [...] à regarder* » : malgré la valeur générée, il n'y a finalement que « *très peu de gens en fait, dans les boîtes autour de l'écosystème, qui sont impliqués dans les couches protocolaires, en tout cas sur Bitcoin [...] Ethereum c'est un peu l'exception avec Consensys [(entreprise du co-fondateur d'Ethereum Joe Lubin) et] la fondation Ethereum [en comparaison] Blockstream [...] c'est ce qui pourrait se rapprocher le plus [...]* d'un truc comme l'Ethereum Foundation dans le monde de Bitcoin » [N. Bacca, Entretien n° 8, rejoint par Léa Thiebaut, Entretien n° 21]. Rapporté à d'autres projets à codes sources ouverts, ce problème structurel s'expliquerait par l'absence d'« *une culture qui va fonctionner un petit peu comme tu peux avoir sur Linux aujourd'hui. Les choses s'y sont extrêmement professionnalisées et au final tu as toutes les grandes distributions qui participent aussi au noyau. Tu n'as pas du tout cette équivalence en fait aujourd'hui dans les cryptomonnaies**. Donc tu as extrêmement peu [...] de développeurs* Bitcoin sur le... au niveau du protocole et du consensus qui sont dans une boîte. » [N. Bacca, Entretien n° 8] Ainsi, la grande majorité du financement « *envers les devs provient de propositions d'emploi [et de] systèmes de bourse ou de sponsor, ce qui me plaît énormément en fait. Moi j'aime bien ce côté indépendance [...] des Devs* ».

Une telle situation pose des questions. Si l'établissement de « *la hauteur des passerelles** à l'intérieur du parc de Long Island a été choisie afin d'interdire le passage des cars, moyen de transport privilégié des Noirs, de telle sorte que la fréquentation de ces zones de loisir reste l'apanage des Blancs » (Akrich 2010, p. 219, note 1), que dire du design d'un système monétaire, même distribué et du rôle de ces concepteurs⁴¹⁶ : Bitcoin ? « *Évidemment que c'est politique [et] il faut être un petit peu naïf pour considérer que ça ne l'est pas* », impossible de ne pas reconnaître des « *enjeux politiques [et] de gouvernance au sens large* » dans cette situation. « *Cela soulève des questions sur leur neutralité* » et la présence de conflits d'intérêts potentiels : « *comment cela se passe si [...] une idée pour améliorer le protocole Bitcoin [implique de rendre] incompatible, voire obsolète tous les produits issus d'une de ces entreprises [...]. Viendrait[-on] à discuter de cette mise à jour [...] ou pas ? Je ne dis absolument pas [que ces conflits d'intérêts existent] mais [...] c'est des questionnements qui sont ouverts.* » [L. Thiébault Entretien n° 21] A. Walch a questionné sur Twitter cette neutralité⁴¹⁷ : « *Serait-ce un problème si [Chaincode Labs] ou toute autre entité payant les développeurs* principaux #Bitcoin ont tenté d'influencer le développement ? Et s'ils menaçaient de licencier les développeurs* principaux qu'ils paient à moins que les développeurs* ne préconisent une trajectoire particulière pour le protocole ? Le développeur* devrait-il divulguer publiquement cette pression ? Quelles attentes ont les gens par rapport à un tel scénario ?* ». Le CEO de Blockstream, A. Back, assurera que non, leur indépendance est formellement garantie : « *À [Blockstream] nous avons négocié avec des investisseurs pour l'indépendance des développeurs* de bitcoins. Si une nouvelle direction essayait de faire pression sur un développeur* principal pour qu'il apporte un changement qu'il jugeait mauvais pour Bitcoin, il pourrait démissionner et l'entreprise serait tenue de payer un an de salaire pendant qu'il trouve un nouveau financement [. J]e pense [Digital Currency Initiative] et peut-être [Chaincode Labs] doivent avoir quelque chose de similaire (mais probablement sans parachute). Il existe également quelques développeurs* indépendants "no strings" financés par des bourses. [...] Je sais qu' [Angela_Walch] semble essayer de construire un argument sur la centralisation du contrôle[...]. Mais les gens ont 5 ans*

⁴¹⁶ Léa Thiebault, en explicitant le « *Slogan Code is Law* », fait référence au texte de Lessig et à l'exemple de la construction d'un pont dont le design servait des fins racistes. Sans trouver cette référence dans le texte cité, nous reconnaissons les travaux de L. Winner (cité par Akrich 2010).

⁴¹⁷ https://twitter.com/angela_walch/status/1230239961045241856

et https://twitter.com/angela_walch/status/1230239962336985093 [Consultation au 24/06/2023].

*d'avance pour reconnaître et se défendre contre de tels risques. Et il y a des expériences antérieures à #bitcoin dans les FOSS [et puis] les gens ne sont pas très motivés par le salaire : ils sont poussés à travailler sur des choses utiles à la société, et non sur des choses qu'ils considèrent comme défiant l'éthique »*⁴¹⁸. A. Back reproche à Walch de chercher par ces questions à dresser l'image d'une gouvernance de Bitcoin centralisée, comme pour démontrer que de ne pas parler de politique de Bitcoin relèverait moins de la naïveté que d'une invisibilisation stratégique : les crises révèlent au grand jour ce qui, pour certains *bitcoiners**, relève de « *tabous [et de] questions qui ne sont pas posées !* » [L. Thiébaut, Entretien n°21]. Il ne faudrait pas s'aventurer à le faire (cf. Non-Entretien n°27). D'autres *coincers** considèrent que ces stratégies d'évitement et d'occultation de la gouvernance des CM prive leur développement d'un professionnalisme et d'une transparence nécessaires : il faut « *faire en sorte de créer un écosystème qui soit plutôt défavorable [aux conflits d'intérêts]. Après heureusement qu'il y a ces entreprises dans l'écosystème[,] c'est incroyable ce qu'ils font ! Le tout c'est de trouver en fait une sorte d'éthique de communauté [comme] pour Linux cela ne s'est pas créé non plus en une journée* » [L. Thiébault, Entretien n° 21, rejoint par Bacca, Entretien n° 8]. Selon ce prisme, la méconnaissance par le grand public de ces crises est en partie le produit d'une faible publicité servant à cacher une gouvernance moins *invisible* qu'indicible.

Cette fragilité ontologique (perçue ou non des *bitcoiners**) se lit aussi dans le répertoire logiciel « Bitcoin Core » qui témoigne de l'activité de maintenance quotidienne⁴¹⁹. Cet arrangement sociotechnique clef de l'administration des codes logiciels Bitcoin Core permet d'établir tout à la fois les rôles et statuts de « Core Dev », le cadre de cette activité de production, et les dispositifs de contrôle et de consignation assurant traçabilité, transparence et auditabilité en vue d'information communautaire.

III.2.2 Où modifier Bitcoin ? Un « repo Bitcoin Core » encadré et hiérarchisé

Codes et codeurs apparaissent centraux lors des crises, comme pour le fonctionnement routinier de Bitcoin. Leur mise en relation nécessite un lieu et des modalités d'interactions. Cette activité de production des codes d'une CM est hautement critique, et les modifications de code sont précisément encadrées. Ces dispositifs d'encadrement renvoient à un lieu particulier qu'il nous faut présenter.

Le répertoire « Bitcoin Core » et son administration

L'espace ordonné du face-à-face entre codes et codeurs, central tant dans les mises en crise que dans les remises en ordre, est la forge logicielle* « Github » (voir Encadré n°5 suivant), la plateforme d'hébergement référente du répertoire logiciel « Bitcoin Core » (le « *repo* »). Le type de dispositif qu'est une forge n'est pas spécifique au développement de CM, mais emprunté au champ de la production de logiciels libres et ouverts, dans lequel Nakamoto s'inscrit (Cf. Chap. I).

⁴¹⁸

Voir

<https://twitter.com/adam3us/status/1233309387646697483>;

<https://twitter.com/adam3us/status/1233310168831709186>

<https://twitter.com/adam3us/status/1233310814783844352> <https://twitter.com/adam3us/status/1233311769692721158> [Consultation au 24/06/2023].

⁴¹⁹ <https://github.com/bitcoin/bitcoin/graphs/contributors?from=2009-10-14&to=2021-10-21&type=c> permet d'observer l'activité sur le répertoire logiciel « Bitcoin Core » [consultation au 14/10/2021].

Encadré n°5 : Les forges logicielles, un système de production collaboratif de logiciels libres

Le développement logiciel de Bitcoin et des CM repose sur la création distribuée de ressources. L'agrégation de contributions librement accessibles y suit un « *modèle d'action collective et de production de biens publics qui intègre l'utilisation de réseaux* de communication numérique et des technologies de l'information* » (Benkler 2006 cité par Shaw et Hill 2014). Les objectifs de la liberté logicielle, tels que définis par Stallman (1999 ; cf. Chap. I), nécessitaient des moyens. Apparues à « *la faveur de l'accès public à l'Internet [...] des années 1990* », les forges logicielles sont de ceux-ci, en tant qu'environnements de développement logiciel collaboratif (Elie 2013). Leur développement s'est fait en trois temps. Le premier est celui du « *free software* », où une « *communauté proche de l'esprit académique [valorisant] l'efficacité de la coopétition* » (Elie 2013) est intéressée par la production de savoir mais non par la vente, d'où la création d'outils libérant « *les couches basses de l'informatique [...] les couches systèmes et réseaux** » (protocole IP de V.Cerf et B. Kahn en 1974, ou http, de T.B. Lee ; *Ibid.*). Le tournant 2000 correspond au « *moment open source* » (*Ibid.*) à la tête duquel sont des industriels. Produisant pour vendre, ils reconnaissent l'efficacité de la collaboration (exemple de la fondation Apache), et cela va conduire au développement de logiciel de plus haut niveau et à une meilleure interopérabilité. C'est l'absence de répercussion pour les utilisateurs de ces logiciels qui les poussera à se constituer en une troisième communauté. Les utilisateurs se mettent à « *gouverner la production, [...] piloter la feuille de route des logiciels qu'ils utilisent et achètent, en particulier les logiciels métier* » (*Ibid.*, p. 12). Ces temps et communautés ont développé des dispositifs qui, bien qu'*ad hoc*, « *convergent vers les mêmes outils de production* » (*Ibid.*, p. 15). La forge logicielle* « *Github* » est une héritière de cette convergence et ces anciennes communautés y cohabitent aujourd'hui (McMillan 2012).

Les forges contemporaines sont tout à la fois des plateformes d'hébergement web pour les codes sources logiciels, un ensemble d'outils de développement logiciel et des plateformes de discussion et d'échange pour les contributeurs. Portail communautaire accessible via un site Internet, elles offrent une série de services de gestion de projet, avec : un système de gestion des versions (de type Git ou mercurial) ; des systèmes de *tracker*, pour faire remonter les demandes de fonctionnalité, gérer l'attribution et le suivi des bogues, ou encore la gestion/répartition des tâches ; un service de publication/livraison des paquets et fichiers (nous verrons que les *bitcoiners** innovent dans ce domaine) ; des outils d'intégration continue ; des gestionnaires de listes de discussion (et/ou forums) et de documentation (de type wiki) permettant les discussions et échanges d'information entre les participants (Creatis 2017). Ces outils et procédures normalisés permettent, en les encadrant, la production/gestion de codes sources logiciels. L'administration du répertoire d'un logiciel repose sur une pyramide hiérarchisée de droits. Sont formellement définis des statuts, des rôles et des niveaux de priviléges, des plus réduits aux plus étendus (dans l'ordre, « *read* », « *triage* », « *write* », « *maintain* » et « *admin* ») dessinant une configuration particulière des sept « *faisceaux de droits* » d'Hess et Ostrom 2007, déjà présentés (cf. Chap. II, section II.3.3 ; voir Tableau 7 suivant concernant l'administration de Bitcoin Core). Au sommet, les « *maintainers* » jouissent de tous les droits : contrôlant l'accès aux droits et permissions, ce sont les seuls à pouvoir ajouter, supprimer ou promouvoir d'autres membres à différentes positions ; ils peuvent changer le nom et la description de l'équipe ; éditer/supprimer des discussions, etc. Ainsi, si tout un chacun est théoriquement libre de Fork*er un répertoire, c'est-à-dire de créer une nouvelle branche, produire un correctif et proposer sa fusion dans la branche principale (« *Pull Requests* » ou demande d'extraction), l'implémentation dans les codes suit des procédures définies (cf. section 1.2.3 suivante), qu'entérinent ou non les *administrateurs** disposant des droits associés (« *commit right* » & « *merge* ») via *commit* (cf. sauvegarde constituant une étape du développement de la version). L'encadrement est à la fois formel et informel, puisqu'au droit d'administration s'ajoutent des ordres de statuts où la réputation, jamais stabilisée, est primordiale (Stewart 2005). Formellement ouvertes, ces plateformes le sont moins pratiquement : aux compétences impliquées d'écriture de codes s'ajoute une maîtrise des différents outils à disposition (Git, etc.) et du jargon associé (« *ACK* » pour « *Acknowledge* », « *utACK* » pour « *Untested Acknowledge* », « *NACK* » pour « *No Acknowledge* », « *RFC* » pour « *Request for Comment* », etc.⁴²⁰). Ces communautés de production distribuée tendent à se présenter comme des « *oligarchies* » aux « *élites et [...] leaders puissants* », contredisant « *l'idée qu'[elles] impliquent des formes organisationnelles démocratiques* » en soi.

Aujourd'hui, au sein du « repo Bitcoin Core » est hébergée la majorité des activités entourant la production des codes sources de Bitcoin Core. Les *bitcoiners** y trouvent un lieu d'hébergement des différentes versions logicielles, un ensemble d'outils de développement et un lieu de communication entre développeurs*. La forge leur permet d'encadrer de manière procédurale et ordonnée les interactions des acteurs, que ce soit par les dispositifs génériques offerts par la

⁴²⁰ Voir <https://docs.github.com/en/get-started/quickstart/github-glossary> [consultation au 18/11/2021].

plateforme, ou par ceux spécifiquement développés par les *bitcoiners**. Mais cette situation n'a pas toujours existé. Nakamoto « était un codeur brillant » mais « excentrique » (G. Andresen cité par Simonite 2014), maîtrisant peu les outils de gestion logicielle moderne de ce type : loin des standards logiciels, les codes originaux prenaient la forme d'« une énorme base de code désordonnée » (McCormack et Corallo 2019). M. Corallo abonde en soulignant le travail déjà accompli et celui qu'il reste à faire : « le logiciel original de Bitcoin était très monolithique. Il était très... Tout le code est dans un seul fichier. Le truc du portefeuille pour les utilisateurs interagit fortement avec le code de validation* et le code de consensus. C'est devenu beaucoup mieux. Nous l'avons beaucoup nettoyé. La séparation entre les différentes parties de Bitcoin Core s'est considérablement améliorée au fil des ans. Il y a encore du chemin à parcourir. Rien n'est parfait, et il y a encore beaucoup de nettoyages et de compartimentages que les gens veulent faire, et cela continuera à se produire lentement [...] en fin de compte, nous avons beaucoup appris et nous avons tellement amélioré le logiciel au fil des ans » [Entretien n° 15]. Comme le chapitre I l'a présenté, au départ Nakamoto coordonne les efforts de développement par mail, puis M. Malmi va créer le « dépôt subversion » de « Bitcoin sur SourceForge », lui-même migré sur GitHub en 2011 (Lopp 2018) pour offrir un espace plus ordonné mais aussi distribué au développement des codes logiciels Bitcoin.

Sur GitHub, le répertoire Bitcoin Core est public, donc « ouvert à tous ». Mais la liberté formelle de contribuer est cadrée par différents dispositifs. Il est attendu pour commencer des volontaires qu'ils respectent un code de conduite stipulant les « comportements acceptables » et « inacceptables »⁴²¹. Ce code de conduite des *bitcoiners** est lui-même évalué (positivement) au regard des standards de la plateforme GitHub (servant à évaluer les projets et leurs mainteneurs)⁴²², et sera clarifié et sanctionné par les mainteneurs du répertoire (« Project maintainers ») et les contributeurs en temps voulu. Les contributions, quant à elles, recouvrent des activités très hétérogènes, allant de simples traductions à des propositions d'innovation dans les codes. Une nomenclature identifie cinq catégories pour lesquelles sont définis des attendus formels, permettant aux volontaires de facilement définir leur niveau d'engagement, selon leur motivation et leur disposition en capitaux culturels (voir le Tableau 6 ci-après).

⁴²¹ Voir https://github.com/bitcoin-dot-org/developer.bitcoin.org/blob/master/CODE_OF_CONDUCT.md [consultation au 25/11/2021].

⁴²² Le respect de ces standards, la présence d'un code de conduite, ou l'existence de règles de contribution sont présentés (absent ou présent) pour tout projet déposé sur Github dans un onglet spécifique des « Insights ». S'y trouvent de nombreuses informations sur les activités hébergées sur le répertoire en question. Pour Bitcoin Core, voir <https://github.com/bitcoin/bitcoin/community> [consultation au 25/11/2021].

Tableau 6 : Nomenclature des contributions possibles aux répertoires « Bitcoin Core »

Type de contribution ⁴²³	Type de procédure et attendu(s) des contributions
Rapport de Bogue	<p>Le signalement de bogue renvoie à deux procédures distinctes :</p> <p>(i) La « divulgation responsable » pour les bogues de sécurité. Elle doit être réalisée en privé, via la « page de contact de sécurité ».</p> <p>(ii) Le « suivi des problèmes publics » (pour les autres bogues). Le contributeur doit rechercher des « problèmes » similaires à ceux rencontrés pour les y incorporer, ou ouvrir un « nouveau problème », en produisant les informations nécessaires⁴²⁴.</p>
Code	<p>Écrire et relire les propositions de modification du logiciel « Bitcoin Core » : les développeurs* se voient proposer deux types d'activités^o:</p> <p>(1) Rédaction : en veillant « <i>à fournir un code de bonne qualité et à respecter toutes les directives</i> » décrites dans un fichier du répertoire ;</p> <p>(2) Audit : les « développeurs* expérimentés » peuvent examiner les modifications de code reçues.</p> <p>Sont aussi listés : des problèmes en attente de correctifs et des procédures de test à développer.</p>
Documentation	Écrire la documentation (utilisateurs et développeurs*) : amélioration de la documentation disponible (corriger les incohérences de terminologie, de style, mettre à jour, etc.) suivant un guide stylistique et deux procédures : ouverture d'un nouveau problème (« <i>new issue</i> ») ou d'une demande d'extraction (« <i>Pull Request</i> »).
Traduction	Travaux de traduction pour l'interface utilisateur : les contributeurs doivent créer un compte « Transifex » avant de se rendre sur la page web traduction de « Bitcoin Core » où ils devront s'inscrire. Ensuite, ils peuvent choisir leur langue et proposer des traductions qui, une fois acceptées, seront intégrées à la nouvelle version logicielle.
Support technique	Offrir un support aux autres utilisateurs : aider les utilisateurs débutants en répondant aux demandes en ligne ; à cette fin, sont répertoriés les sites et forums informatifs utiles, et leur niveau d'accessibilité.

Source : Rolland Maël

⁴²³ Pour une présentation générale, voir <https://bitcoin.org/en/bitcoin-core/contribute/>; chaque activité est décrite dans une page dédiée : Rapport de bogue, voir <https://bitcoin.org/en/bitcoin-core/contribute/issues> ; Code, voir <https://bitcoin.org/en/development> ; Documentation, voir <https://github.com/bitcoin-dot-org/developer.bitcoin.org> ; Traduction, voir <https://bitcoin.org/en/bitcoin-core/contribute/translations> ; Support technique, voir <https://bitcoin.org/en/bitcoin-core/contribute/support> [consultation au 25/11/2021].

⁴²⁴ Les contributeurs sont invités à suivre les recommandations générales stipulées dans la documentation de Mozilla. La documentation « Bitcoin Core » précise que sont attendus : une description claire du problème, voire une description des conditions de sa reproduction ; la version « Bitcoin Core » utilisée ou le « commit » utilisé pour sa construction (git log -1), ainsi que les éventuels correctifs appliqués ; enfin, le contributeur peut ajouter toute entrée pertinente de son fichier « debug.log » (en faisant attention aux informations privées qu'il peut contenir). Voir <https://bitcoin.org/en/bitcoin-core/contribute/issues> [consultation au 25/11/2021].

Ces intitulés et leur attendus dessinent une grammaire institutionnelle (Ostrom 2005) permettant de mieux comprendre la diversité des interactions des *bitcoiners** au sein du « repo Bitcoin Core » : des règles, normes et stratégies partagées se distinguent à travers ces attendus plus ou moins prescriptifs (on retrouve les différents types d'opérateurs logiques - « doit », « requiert », « interdit », « permet » - qui les caractérisent, Ostrom et Basurto 2013, p. 11). À leur lecture, on comprend que ces activités reposent sur des compétences, savoir et savoir-faire différenciés : les *bitcoiners** réalisant des traductions sont différents de ceux qui rédigent les rapports de bogue, de ceux qui s'occupent de la rédaction de nouveaux codes ou en réalisent les audits et relectures. Aussi, les membres de la communauté Bitcoin participant à ce type d'activité sont peu nombreux. Si Bitcoin Core, en tant que projet open source* suit un modèle de contribution ouverte, où tout un chacun peut proposer une évolution, l'administration de son répertoire, elle, relève d'une poignée d'acteurs désignés, qui ont le pouvoir de les approuver et de les intégrer dans une nouvelle version.

D'une hiérarchie formelle selon le principe « du moindre privilège » à la désignation informelle des mainteneurs « Core »

Le chapitre II a conclu que la gouvernance d'une CM comme Bitcoin se présentait comme polycentrique : en tant que système de ressources, une CM est constituée de sous-systèmes de ressources propres, articulés entre eux (Hess et Ostrom 2003 ; cf. Chap. II, section II.3.3). Le répertoire Bitcoin Core GitHub constitue l'un de ces sous-systèmes essentiels de l'infrastructure Bitcoin et les « unités de ressources » produites et distribuées, bien qu'immatérielles (les *codes open source** et les informations les concernant) n'en sont pas moins critiques. Aussi, ce système et son administration sont fortement régulés. Ces régulations renvoient à la présence des sept composantes

structurelles⁴²⁵ qui, dans le cadre IAD d’Ostrom, s’articulent singulièrement pour définir le système institutionnel ayant cours dans une arène d’action (Ostrom Bazurto 2011 ; Chanteau et Labrousse, 2013). Cette régulation passe d’abord par l’identification de statuts d’acteurs à rôles spécifiques, comme les « Core Mainteneurs », disposant de priviléges d’administration divers.

Les *bitcoiners** reconnaissent qu’une « *certaine hiérarchie est nécessaire à des fins pratiques* » (Bitcoin Core 2018b⁴²⁶). Elle se justifie par les contraintes de coordination importantes qu’implique la gestion d’une multitude d’activités et d’acteurs : « *si n’importe qui pouvait fusionner dans la branche master, cela [correspondrait] à un scénario du type "trop de cuisiniers dans la cuisine"* » (Lopp 2018), pouvant dégénérer en des corruptions volontaires ou du vandalisme. N’importe qui ne peut pas faire n’importe quoi suivant que l’administration du répertoire Bitcoin Core repose sur une structure hiérarchique formelle avec : « *des "mainteneurs" de répertoire qui sont responsables de la fusion des demandes de retrait [les « Pull Requests »], ainsi qu’un "mainteneur principal" qui est responsable du cycle de publication, de la fusion globale, de la modération et de la nomination des mainteneurs* » (*Ibid.*).

Tableau 7 : Les priviléges d’administration du répertoire Bitcoin core

Privilège / Rôle accessible sur le repo Bitcoin Core ⁴²⁷ (s)	Maint. Princ.	Maint. Simple	Autres contrib.
1 - Lecture (« Read ») <i>Accès à l’information</i>	Oui	Oui	Oui
2 -Triage (« Triage ») <i>Gestion active des problèmes et des PR sans accès en écriture</i>	Oui	Oui	Oui
3 -Écriture (« Write ») <i>Contribution active au code</i>	Oui	Oui	Non
4 - Maintenance (« Maintenance ») <i>Gestion du dépôt sans accès aux actions sensibles ou destructrices</i>	Oui	Oui	Non
5 - Admin (« Admin ») <i>Accès complet au projet, y compris les actions sensibles ou destructrices</i>	Oui	Non	Non

Source : Rolland Maël

L’administration du système de ressources qu’est le « repo Bitcoin Core » relève d’une pyramide de droits, plus ou moins subordonnés, suivant l’application du principe de moindre privilège, devant permettre une gestion efficace, assurant que chaque acteur dispose du niveau d’accès approprié à sa fonction sans lui donner plus de priviléges que nécessaire. En son sein, cinq familles de droit/privilège existent (cf. Tableau 7 ci-contre), chaque niveau ajoutant aux droits précédents de nouveaux droits. On y trouve : la « lecture », qui correspond au rôle par défaut et ses droits afférents permettent de voir et discuter du projet sans contribuer au code - dans l’ordre des faisceaux de droits (Hess et Ostrom 2007, p. 52-53), ce statut recouvre les droits d’accès (tout le monde peut y venir, observer, voire échanger), de prélèvement (rien n’empêche de copier les codes qui s’y trouvent) et de contribution (puisque tous

⁴²⁵ Les sept composantes structurelles d’un système de règles sont : les règles de définition des rôles (ou « position rules ») ; les règles d’accès au rôle (ou « Boundaries rules ») ; les règles d’allocation des ressources (ou « Allocation / choice rules ») ; les règles sur les procédures de décision collective (ou « Aggregation rules ») ; les règles d’information (ou « Information rules ») ; les règles de contribution/rétribution (ou « payoff rules ») ; les règles délimitant les usages possibles des ressources (ou « Scope rules »). Voir Ostrom et Basurto (2013, p. 10-11).

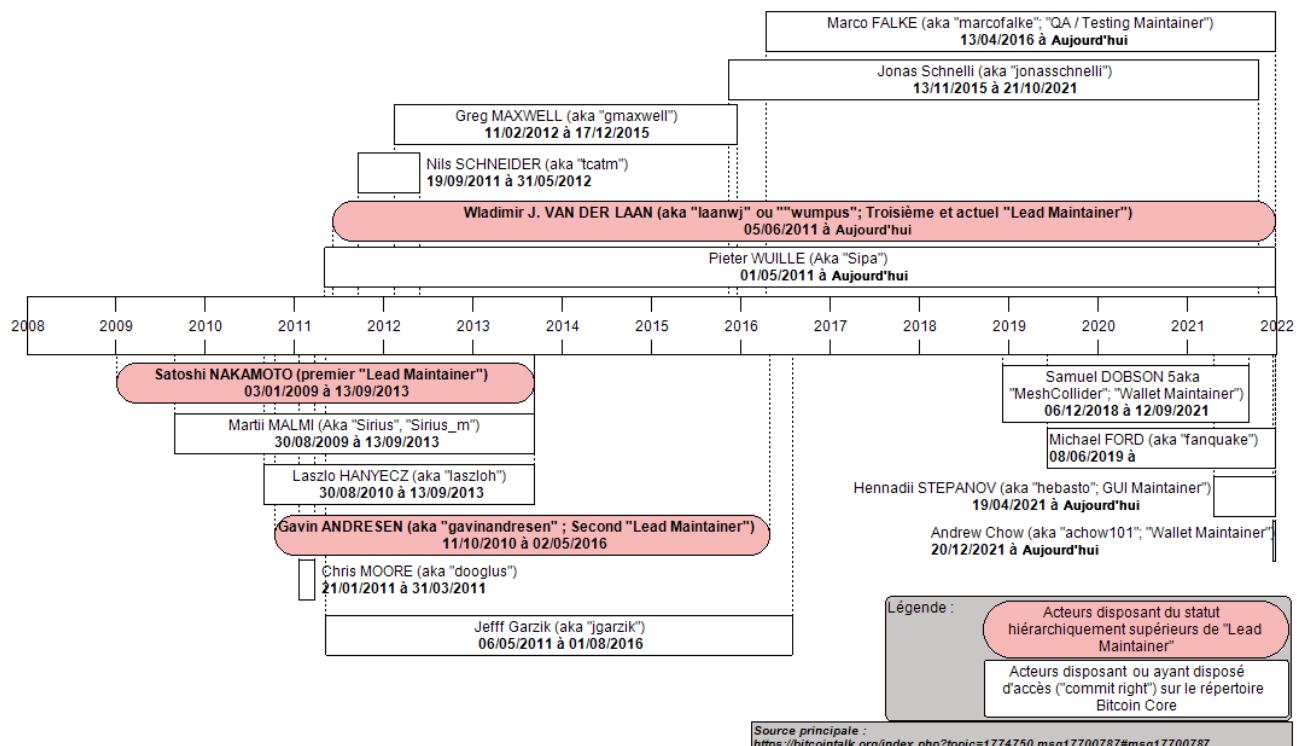
⁴²⁶ <https://github.com/chaintope/tapyrus-core/blob/master/CONTRIBUTING.md> [consultation au 25/11/2021].

⁴²⁷ Nous nous sommes limités aux catégories génériques, au sein de chacune se trouve une multiplicité de combinaisons de priviléges et d’actions potentielles, voir <https://docs.github.com/en/organizations/managing-access-to-your-organizations-repositories/repository-permission-levels-for-an-organization> [consultation au 29/11/2021].

ici peuvent se lancer dans des propositions) ; le « triage » ajoute aux droits précédents des droits liés à la gestion active des problèmes et des « *Pull Requests* » sans pour autant avoir un accès en écriture ; l’« écriture » et ses priviléges, plus critiques que les précédents rôles, sont réservés aux contributeurs actifs et reconnus. Ce rôle ajoute aux droits précédents des droits de management et de gestion ; la « maintenance » va encore plus loin : ces droits permettent de gérer le dépôt, mais aussi l'accès aux actions sensibles ou destructrices n'est pas donné. Ici comme précédemment, on trouve des acteurs reconnus, de type « mainteneurs simples ». Enfin, les droits hiérarchiquement supérieurs d'« Administration », touchant à tout, y compris aux actions sensibles ou destructrices (donc ajoutant aux précédents ceux d'exclusion et de suppression, *Ibid.*), sont le privilège exclusif d'un mainteneur principal unique.

Ce groupe de mainteneurs simple, avec le mainteneur principal au centre, est aussi essentiel que restreint. Depuis 2009, nous avons décompté 16 acteurs ayant tenu ou tenant ce rôle de « mainteneurs » (cf. Chronologie 5 suivante). Le nombre de développeurs* dits « Core Devs » excède ce décompte, car il est construit à partir de l'organigramme général du repo Bitcoin Core : sont exclus les contributeurs actifs et reconnus qui, à la manière d'un acteur aussi central que M. Corallo, disposent de priviléges en lien avec leur activité, sans pour autant porter la casquette de mainteneur simple. Dans tous les cas, l'usage de priviléges d'administration et de gestion donne lieu à consignation en vue de traçabilité et d'information.

Chronologie 5 : Les différents acteurs disposant ou ayant disposé de droits spécifiques d'accès (« commit right ») et du rôle de « Core Mainteneurs » sur le répertoire Bitcoin Core



Source : Rolland Maël

Au sommet de la hiérarchie, le « mainteneur principal » jouit des rôles d'« *Admin* », donc, de la plénitude des priviléges et pouvoirs offerts par la plateforme. Trois individus se sont succédé à

ce rôle depuis 2009 : S. Nakamoto, qui fut remplacé par G. Andresen, lui-même remplacé par W.J. van der Laan, mainteneur principal actuel. Au niveau intermédiaire, on trouve les « mainteneurs simples » et les « Core Devs » à la Corallo, qui disposent à différents degrés (en fonction de leurs activités), des priviléges afférents aux rôles de « *triage* », d’« *écriture* » et de « *maintenance* », comme le droit d’administration (ou « *commit right* ») sur tout ou partie (« *portefeuille* », « *questions/réponses et testing* », etc.) du répertoire Bitcoin Core. Le dernier niveau correspond au commun des utilisateurs, avec le rôle par défaut de « *lecture* ». Toute contribution émanant de la base se doit d’être avalisée par un échelon supérieur. Le droit à proposition d’évolution des codes est donc suspendu à l’aval des « mainteneurs simples » ou du « mainteneur principal ». Ce sont eux qui, *in fine*, ont le pouvoir de les accepter et de les intégrer dans les codes d’une nouvelle version. Au sommet de la pyramide, le « mainteneur principal » peut, comme tout mainteneur simple, être appelé à accepter/refuser des modifications proposées par la base, mais son rôle est de superviser l’ensemble des aspects du projet et d’être « *responsable de la coordination des versions* » (Lopp 2018). Il jouit d’un pouvoir discrétionnaire sur les codes sources ou sur les nominations/révocations des autres mainteneurs.

Si les droits sur le répertoire Bitcoin Core sont formels, les dispositifs et critères présidant à la désignation de ces acteurs clefs sont, eux, informels. Comme souvent dans les communautés open source, cette désignation relèverait « *de la méritocratie, où les contributeurs à long terme gagnent davantage la confiance de la communauté des développeurs** » (Bitcoin Core 2018b). La désignation des mainteneurs « Bitcoin Core » relève de la pratique, sans qu’aucun critère, ni processus formel de désignation ne soit explicité, ni publicisé. Cette élection concernerait « *des contributeurs qui ont construit un capital social suffisant au sein du projet en apportant des contributions de qualité sur une période donnée* » (Lopp 2018). Elle apparaît fondée sur un mécanisme de cooptation donnant un poids important aux affinités électives, aux proximités sociales, aux relations de confiance de long terme, donc à une certaine homogénéité en valeurs. Que ce soit pour le statut de « mainteneur principal », qui a été « *transmis volontairement au fil des ans* » (*Ibid.*), ou pour les « mainteneurs simples », qui sont nommés par « *le groupe existant de mainteneurs* », décidant discrétionnairement « *d'étendre le rôle à un contributeur qui a fait preuve de compétence, de fiabilité et de motivation dans un certain domaine* » en lui accordant « *un accès de commit au compte GitHub* » (Lopp 2018). Et il faut que le mainteneur principal accepte, car, en dernière instance, il est le seul à pouvoir donner ou reprendre les droits d'accès à un compte « *Github* ».

Est-ce à dire que le « mainteneur principal » est un dictateur qui, « *éclairé* » ou non, fait ce qui lui plaît ? Cela interroge le cadre des relations entre le « mainteneur principal » et les « mainteneurs simples » et, finalement, les modalités des prises de décision. Il ressort de ce dispositif un cadre ni transparent, ni fixé une fois pour toutes, qui évolue suivant la personnalité du « mainteneur principal », soulignant du même coup le poids pris par ce rôle et l’acteur qui le tient. Au commencement de Bitcoin, l’administration des codes relevait d’une logique de « *dictateur éclairé* » et « *tout était vraiment plus simple [...] : on avait un code source et une personne sous pseudonyme qui prenait toutes les décisions [...]* » (Andresen cité par Ailleurs 2015). Suite au retrait de Nakamoto et sa transmission des priviléges d’administration à Andresen, ce dernier va « *essayer de décentraliser tout cela* » en établissant cinq autres mainteneurs à ses côtés⁴²⁸ (*Ibid.*). Décentralisation pour le moins relative, car Andresen le concède, en l’absence de consensus : « *je tranchais. Je décidais d'aller dans une direction plutôt qu'une autre. J'agissais comme un dictateur bienveillant pour Bitcoin Core mais je pense que cela marchait.* » (*Ibid.*). Preuve encore du poids pris par la personnalité du mainteneur principal, cette situation va changer à partir de 2014, avec

⁴²⁸ Wladimir J. van der Laan, Gavin Andresen, Jeff Garzik, Gregory Maxwell et Pieter Wuille.

l'arrivée de W.J. van der Laan : « *Wladimir, à qui j'ai passé la main, n'envisage pas son rôle ainsi. Il est plus conservateur, il n'ajouterait rien sans avoir le consensus* [des autres mainteneurs⁴²⁹]. *Les changements peuvent donc être bloqués par un simple veto et je ne pense pas que cela soit très sain.* » (*Ibid.*). W.J. van der Laan conçoit son rôle de « mainteneur principal » du répertoire « Bitcoin Core » différemment et souhaite défendre « *avec ferveur la décentralisation et l'autonomie* » de Bitcoin, d'où des actions mues par un principe simple : « *toute proposition ou amélioration survenant dans un BIP au profit de Bitcoin doit être approuvée par la grande majorité des développeurs* et des collaborateurs avant d'être mise en œuvre dans le système* » (Bit2MeAcademy 2020). D'ailleurs, ce groupe n'est ni totalement fixe, ni totalement homogène. Au contraire, l'histoire démontre qu'il est en perpétuel recomposition et que, entre les acteurs concernés existent des différences de vues présidant à l'existence de conflits, parfois violents, comme le « Scaling Debate » en a témoigné.

Une technocratie soumise à consensus communautaire : entre confiance et défiance

Malgré la décentralisation vantée de Bitcoin, ce dernier repose sur une implémentation logicielle référente et la maintenance de ces codes nécessite un groupe restreint et centralisé d'acteurs. Ce centre peut prendre un poids considérable, selon qu'il se comporte ou non comme dictateur philosophe. Et tous voient leur activité de production dépendre de la plateforme « GitHub ». Ces acteurs nécessaires disposent d'un pouvoir structurel que les *bitcoiners** reconnaissent comme problématique. D'un côté, « *dans une perspective adverse, on ne peut pas faire confiance à GitHub* » puisque ces employés « *pourraient utiliser leurs priviléges administratifs pour injecter du code dans le dépôt sans le consentement des mainteneurs* » (Lopp 2018). D'un autre, « *la question de savoir qui contrôle la capacité à fusionner les modifications du code dans le dépôt GitHub de Bitcoin Core* » revient de manière récurrente sous la forme d'« *un "point central de contrôle" du protocole Bitcoin* » (*Ibid.*). Cette centralisation fait peser des risques importants sur Bitcoin et pourrait conduire à des « *scénarii catastrophes* » (Hasday 2020). Qu'est-ce qui empêcherait qu'un des mainteneurs décide de saboter le code du Bitcoin Core dont il a la charge ? Ou qu'un attaquant prenne le contrôle d'un compte de mainteneur afin, là encore, de saboter ces codes pour tuer Bitcoin ? D'ailleurs, les mainteneurs doivent-ils faire confiance à l'entreprise GitHub et ses employés pour ne jamais modifier arbitrairement le repo Bitcoin Core et ce qui s'y trouve ? Cette poignée de développeurs* hautement qualifiés et d'ingénieurs informatiques ayant la charge de faire évoluer l'infrastructure Bitcoin peut apparaître comme constituant une structure de gouvernance hautement technocratique, fondée sur l'autorité d'un leader charismatique (De Filippi et Loveluck 2016, p. 15).

Lopp (2018) répond que, « *bien qu'il existe une poignée de comptes "mainteneurs" [...] il s'agit plus d'une fonction de concierge que d'une position de pouvoir* ». La position de surplomb de Bitcoin Core relève d'un point Schelling, il « *est un point central pour le développement du protocole Bitcoin plutôt qu'un point de commande et de contrôle. S'il cessait d'exister pour quelque raison que ce soit, un nouveau point focal émergerait - la plateforme de communication technique sur laquelle il est basé (actuellement le dépôt GitHub) est une question de commodité plutôt qu'une question de définition/d'intégrité du projet. En fait, nous avons déjà vu le point central du développement de Bitcoin changer de plateforme et même de nom* » (*Ibid.*). L'épisode du changement de nom a déjà permis de souligner les vues parfois opposées des « Core Devs » sur les

⁴²⁹ La personne en charge allant jusqu'à influencer le seuil établi du consensus entre mineurs (en part de Hashrate du réseau) nécessaire à l'acceptation d'un Hard Fork : « *Andresen, di[s]ait que 75% des mineurs suffisent [...] tandis que les développeurs* de Bitcoin Core aimeraient voir un "accord quasi-universel"* » (Torpey 2016, cf. section III.3.2 suivante sur ces questions).

objectifs et moyens du développement de Bitcoin. En outre, qu'un consensus émerge entre eux ou non, ces développeurs* devront encore composer avec l'ensemble des *bitcoiners**, qui peuvent adhérer ou non à leurs décisions : en dernière instance, la communauté « *tranche par elle-même* » en mettant à jour ses logiciels ou non. La gouvernance *sur* le protocole de Bitcoin ne se réduit pas aux seuls développeurs* puisqu'il existe un jeu complexe de rapports de force entre les parties en présence, relevant de l'édition de structures de gouvernance visant à réaliser des objectifs collectifs, gérer les conflits et contrôler les relations de pouvoir. C'est ce processus de gouvernance dynamique qui, en assurant la légitimité collective des actions décidées, garantit la stabilité et soutenabilité de Bitcoin.

La légitimité des modifications proposées dépend ultimement du degré de consensus qui les entoure. Au sein des communautés de CM comme Bitcoin, comme pour de nombreux protocoles Internet, cette légitimité relèverait de l'obtention d'un « *consensus approximatif* » (« *rough consensus* ») comme défini par l'« *Internet Engineering Task Force* » (IETF) (*Ibid.*, p. 18; Lopp 2018). Ce type de consensus désigne une prise de décision reposant sur « *le sentiment du groupe concernant une question particulière à l'étude* » qui « *n'exige pas que tous les participants soient d'accord, même si c'est bien sûr préférable* » (Internet Engineering Task Force 2014). Il n'est pas question d'acceptation à la majorité absolue (> 51%). L'« *absence de désaccord est bien plus importante que l'accord* », cette règle « *d'éviter les dangers de la "règle de la majorité" et de parvenir à des décisions consensuelles avec les meilleures résultats techniques* » (*Ibid.*). L'IETF précise qu'il s'agit moins de définir des processus et des procédures que de réfléchir à la façon dont sont prises les décisions (*Ibid.*).

Il nous reste à voir comment la faille Bitcoin CVE 2018 fait apparaître que ce « *consensus approximatif* » en cache différents sous-types, suivant différentes procédures communautaires pour faire évoluer les codes Bitcoin Core. Suivant le périmètre de la modification proposée, des procédures distinctes sont en place, dont les exigences asymétriques forcent à mobiliser des arènes plus ou moins locales afin de toucher tout ou partie des membres de la communauté. Que cette crise ait été déclenchée et résolue sous le sceau du secret met au jour l'existence de niveaux d'engagement variés des parties prenantes à ce consensus, au sein d'arènes de débats segmentées. Ainsi, si les acteurs précédents disposent de pouvoir sur le sous-système du répertoire GitHub « *Bitcoin Core* », les activités qu'ils y réalisent sont encadrées, et de nombreux dispositifs et arrangements visent à garantir une information et un contrôle communautaire en dernier ressort, afin de prévenir tout abus et catastrophe.

En contrepartie des pouvoirs que les mainteneurs se voient octroyer, un système de contrôle et de consignation *ad hoc* a été ajouté à celui fourni par défaut par GitHub, permettant d'assurer la traçabilité, la transparence et l'auditabilité des modifications passées : le « *système d'intégration continu basé sur des vérifications de clefs PGP de confiance* » (Lopp 2018). Il impose que toute modification des codes sources passe par un mainteneur qui doit la signer avec une clé PGP reconnue⁴³⁰. L'identité des mainteneurs Bitcoin Core ayant des droits d'administration est publique,

⁴³⁰ Un « *pre-push hook* » existe pour garantir aux mainteneurs « *qu'ils ne poussent pas de commits non signés dans le dépôt* » et les « *commits de fusion sont optionnellement horodatés de manière sécurisée via OpenTimestamps* » (Lopp 2021). « *OpenTimestamps* » est un service de consignation et d'horodatage* utilisant la base de données Bitcoin, permettant de certifier l'existence de données (dont l'empreinte de hash est consignée) à une date précise (celle de la publication de la transaction).

et s'y attache une clef de chiffrement PGP unique⁴³¹. Toute modification des codes sources Bitcoin doit être signée par une de ces clefs PGP de confiance. Ce dispositif, en plus d'assurer que seuls les mainteneurs peuvent réaliser de telles actions, permet de retracer l'ensemble des évolutions de Bitcoin et de les lier à l'identité des mainteneurs qui y ont pris part. Ce dispositif de consignation n'assure pas en soi une sécurité parfaite : une clef PGP n'est « *pas une preuve d'identité* [, elle] pourrait être compromise et nous ne le saurions pas à moins que le propriétaire initial de la clé ne prévienne les autres mainteneurs » (Lopp 2018). Mais en tant que tel, ce dispositif rend « *plus difficile pour un attaquant d'injecter du code arbitraire* » (*Ibid.*), puisqu'il lui faudrait d'abord prendre le contrôle de ladite clef. À cela s'ajoute que lesdites évolutions de codes sont publiques et soumises à des relecteurs, pouvant être formellement reconnus, là encore afin d'assurer contrôle, traçabilité et responsabilité. En cas de constatation d'activités suspectes, les autres mainteneurs peuvent réagir et revenir aux codes initiaux grâce au système de gestion des versions.

Les dispositifs précédents ne sont pas propres aux *bitcoiners** : ces arrangements et pratiques existent depuis longtemps dans la production de logiciels libres. Mais, du fait de l'importance accordée à la sécurité et à l'intégrité des codes sources pour les membres de la communauté, ces derniers ont innové et offert un nouveau standard (repris par des projets comme TOR, Debian, Mozilla, etc., Wirdum 2018). Pour les *bitcoiners**, c'est la nature ouverte des codes sources qui permet à Bitcoin d'être sécurisé et « sans confiance » (trustless), puisque « *toute personne capable de le lire peut vérifier par elle-même s'il fait ce qu'il est censé faire* » (*Ibid.*). Les codes disponibles sur GitHub sont lisibles, car rédigés dans un langage de haut niveau. Il reste un risque fondamental, touchant tant Bitcoin que l'ensemble de la production de logiciels libres, que le « *code source ouvert n'élimine pas* (*Ibid.*) : la confiance que les utilisateurs accordent au fait que « *le logiciel qu'ils exécutent sur leur ordinateur reflète effectivement le code source ouvert* » (*Ibid.*). Comme l'explique C. Dong, Bitcoin repose sur un environnement existant (Ubuntu) qui amène « à télécharger des binaires opaques et non auditables (en d'autres termes, des "binaires de confiance") [...] ce qui nous expose à des risques de tiers », comme le fait qu'un attaquant pourrait corrompre les binaires exécutables « *de la version Bitcoin Core par une intrusion dans l'infrastructure d'Ubuntu (ou, peut-être simplement en y travaillant)* » (Costea 2019). Supprimer ce risque revient à garantir que les codes qui sont lisibles sur le répertoire Bitcoin Core sont bien ceux que l'on trouve dans les binaires du logiciel téléchargé, illisibles pour les humains. À cette problématique cruciale, la communauté des *bitcoiners** répond par une « *politique de sécurité rigoureuse* » : le « *Gitian Buildind* ». Ce dernier est un logiciel à code source ouvert offrant un « *environnement de construction* » (Wirdum 2018) garantissant la production et la publicisation sécurisée de logiciels : comme « *un "ordinateur dans l'ordinateur" qui fournit un espace virtuel où les binaires peuvent être compilés sans variables* » (Costea 2019). Ainsi, « *Gitian* » garantit que la compilation des binaires est exactement la même « *quel que soit l'ordinateur utilisé* » (Wirdum 2018). Ce processus garantit à tout *coiner* que le logiciel qu'il télécharge et installe sur sa machine correspond en tout point aux codes sources qu'il a audités.

⁴³¹ Sur le « repo Bitcoin Core », nous n'avons pas réussi à trouver en un seul endroit, l'ensemble des acteurs disposant de ces priviléges et leurs clefs PGP à jour, comme souligné par Awemany (2018). Sont présentes les 3 clefs PGP de confiance de W. Van Der Laan, de P. Wuille et de M. Ford (<https://github.com/bitcoin/bitcoin/blob/master/SECURITY.md>). La liste de l'ensemble des développeurs* ayant eu des droits d'administration sur les codes sources Bitcoin put être trouvée sur un forum, voir <https://bitcoin.stackexchange.com/questions/176/is-there-a-list-of-core-bitcoin-committers> [consultation au 02/12/2021].

Mais avant qu'une modification des codes protocolaires Bitcoin n'arrive à l'étape de la production de binaires, il faut encore qu'elle ait été proposée, débattue, évaluée, voire critiquée, et amendée dans le cadre procédural en place, ce que nous étudions maintenant.

II.2.3 Bitcoin CVE 2018 : une gouvernance de huis clos suspendue à l'absence de dissensus public

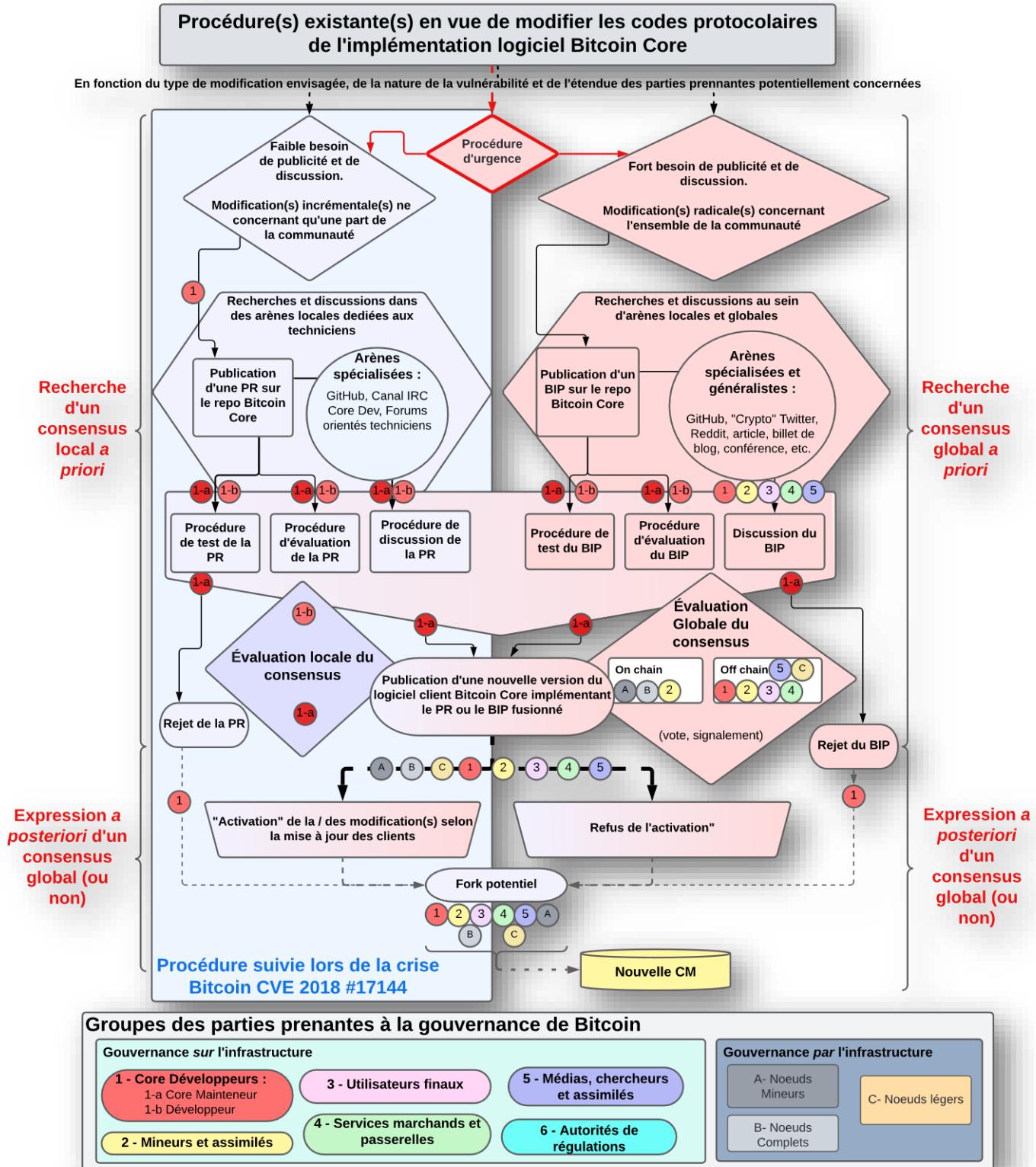
Pour un système de paiement comme Bitcoin, le fait de toucher à ses codes logiciels n'est pas un acte anodin. Nous avons vu que ses codes protocolaires dépendent de l'implémentation « Bitcoin Core », dont l'administration dépend elle-même d'une hiérarchie entre les développeurs* de poids différents, ultimement soumis au pouvoir de la plateforme GitHub. Face aux risques posés par la présence irréductible de tiers de confiance et de priviléges hiérarchiques, des garde-fous communautaires existent. À côté des dispositifs de contrôle et consignation précédemment présentés et au gré des besoins du développement infrastructurel de Bitcoin (comme des crises rencontrées), des dispositifs, procédures et arrangements ont été institutionnalisés pour encadrer le fait de proposer, d'évaluer et de faire valider des propositions de modification des codes sources « Bitcoin Core » et ce, afin de s'assurer de leur innocuité et de construire leur légitimité. Ensemble, ces dispositifs visent à préserver la liberté individuelle des *coiners** quant au choix de l'implémentation logicielle qu'ils font fonctionner, incarnation matérielle et pratique des règles qu'ils considèrent comme canoniques, consensuelles et légitimes (et congruentes avec l'esprit qu'ils en attendent).

Maintenance ou innovation ? Deux procédures d'évolution protocolaire différencierées

Toute proposition, qu'importe sa nature, doit faire consensus en ne produisant pas de divergences d'opinions trop marquées la concernant. Néanmoins, puisque toute modification n'est pas forcément critique, et pour faciliter la maintenance des codes Bitcoin, deux types de procédures ont été mises en place qui n'ont pas les mêmes exigences : la procédure simplifiée des PR, au cœur de la crise CVE 2018, est dédiée aux évolutions considérées comme incrémentales, tandis que la procédure des Propositions d'Amélioration de Bitcoin (ou *BIP* pour « *Bitcoin Improvement Proposal* ») est réservée aux innovations plus radicales [M. Corallo, Entretien n° 15]. Ces deux procédures dessinent une frontière claire entre les modifications proposées selon qu'elles touchent ou non aux règles canoniques consensuelles et, de ce fait, qu'elles concernent tout ou partie de la communauté des utilisateurs. Toucher aux règles de consensus relève d'*« un accord très différent que, par exemple, pour une amélioration des performances de Bitcoin Core »* [Ibid.]. Du fait que chaque procédure vise à produire un consensus mettant aux prises des acteurs, des arènes (plus ou moins locales) et des modalités de publicisation hétérogènes. La Figure 12 présente synthétiquement ces procédures, leurs processus clefs, ainsi que les acteurs impliqués. On trouve les groupes de parties prenantes de la gouvernance de Bitcoin précédemment cernés, que ce soit ceux participant de la gouvernance *par* l'infrastructure (avec les nœuds* mineurs, complets et simples), ou ceux prenant part à la gouvernance *sur* l'infrastructure (en l'espèce les développeurs*, les mineurs et assimilés, les médias et assimilés, les utilisateurs finaux, les services de marchands et passerelles*, et les autorités de régulation ; cf. Chap. II section II. 3.3)⁴³².

⁴³² La granularité est plus faible que celle de la cartographie préliminaire (cf. Figure 7 Chap. II, section II.3.3) : seul le groupe des développeurs* protocolaires, au centre de notre étude, est décomposé en sous-groupes. On le divise entre les « mainteneurs » ayant des priviléges d'administration sur les PR et BIP, et les « développeurs* » qui n'en n'ont pas. Les autorités de régulation ne participent pas. Leur présence en légende ne fait que souligner qu'elles participent du cadre de la décision des acteurs de la gouvernance *sur* l'infrastructure (d'où encadré au fond du même ton).

Figure 12 : Deux procédures différencierées permettant de modifier les codes sources Bitcoin Core



Source : Rolland Maël

La procédure simple des « *Pull Requests* » (demandes d'extraction ou PR) encadre ce qui relèverait de la maintenance des codes protocolaires. Elle est réservée à des changements considérés comme mineurs et peu critiques, au sens où ils ne modifient pas d'éléments relevant des règles de consensus canoniques. De ce fait, ces changements ne concernent qu'une part des utilisateurs sans avoir de conséquence pour « *l'utilisateur moyen de bitcoin* » [M. Corallo, Entretien n° 15]. Le simple usager n'a aucune raison « *de se soucier de l'amélioration des performances de Bitcoin Core, ou même d'un changement d'API [ou] dans l'interface RPC de Bitcoin Core* », ces composants n'étant utilisés que par un collège restreint de super utilisateurs (les « *ingénieurs logiciels travaillant sur Bitcoin Core* » [*Ibid.*]). Tout contributeur au « *repo Bitcoin Core* » (mainteneurs ou non, 1-a et 1-b dans le schéma) peut ouvrir une PR afin de proposer des évolutions incrémentales de code. Sous réserve qu'elles en respectent les attendus formels et convainquent de leur bien-fondé les participants à la discussion, ces PR se satisfont d'un consensus local entre développeurs*. Sans opposition, elles seront implémentées dans une nouvelle version par un « *mainteneur* ». Cette procédure est censée couvrir des modifications non ou faiblement controversées et conflictuelles : « *Vous savez, s'il y a un problème [concernant l'un de ces composants], nous le changeons. Qui s'en soucie ? Alors que, s'il y a un changement dans les règles de consensus [qui] affecte fondamentalement chaque utilisateur de Bitcoin [...] il est important que Bitcoin ait une sorte de processus de changement de consensus orienté vers la communauté* » [M. Corallo, Entretien n°15]. Aussi, la procédure ne prévoit pas de débat et publicisation spécifique autre que celles disponibles sur le « *repo Bitcoin Core* » GitHub et au sein d'arènes de discussion des techniciens (forums, canal IRC dédié, etc.). Une fois publiée, la nouvelle version est soumise à l'expression d'un consensus global : entre opérateurs de nœuds* (mineurs et complets, A, 2 et B dans le schéma) qui mettent à jour (ou non) leur logiciel client et, plus globalement (et indirectement), entre les composantes communautaires (1, 3, 4 et 5) qui utilisent des nœuds* légers (C) et délèguent donc cette mise à jour à des intermédiaires.

La deuxième procédure, celle du « *Bitcoin Improvement Proposal* », vise à encadrer l'ensemble des modifications de codes non couvertes par la procédure simplifiée précédente, c'est-à-dire les modifications protocolaires radicalement innovantes. Contrairement aux modifications incrémentales, elles sont considérées comme relativement « *critiques* », car elles touchent aux règles de consensus canoniques consensuelles : « *un utilisateur de Bitcoin [a] fondamentalement opté pour les règles de consensus de Bitcoin telles qu'elles existent* » *a priori* [M. Corallo, Entretien n°15]. Modifier ces règles est problématique. Au sein de ce type de modification, et suite à un travail de normalisation et de classification (Andresen 2012; Timón 2015; Lombrozo 2015; Lombrozo 2017), les *coiners** distinguent (et préfèrent) les modifications étiquetée *Soft Fork**, conçues comme rétrocompatibles avec les règles canoniques initiales qu'elles remplacent, à celles qualifiées de *Hard Fork**, qui doivent s'imposer à l'ensemble des nœuds* car non rétrocompatibles (cf. section III.3.3). Ces propositions de modifications protocolaires sont en elles-mêmes des crises (de plus ou moins grande intensité) où des *coiners** proposent de remplacer « *Bitcoin* » par « *un nouveau Bitcoin* » aux caractéristiques différentes : s'y s'objectivent les attentes et désirs de tout ou partie de la communauté des *coiners** et l'existence d'une gouvernance politique, qui réussit ou non à modifier cette gouvernance *par l'infrastructure*, *via la gouvernance sur l'infrastructure*. Car, si le WP* décrit le consensus *par le protocole* au centre duquel Nakamoto a établi « *la preuve de travail** [comme] *un moyen de conserver [un] consensus* », Nakamoto ne « *définit pas un moyen de transiter vers un autre consensus, c'est pas décrit cela en fait [...]* Il n'y a pas de specs d'évolution d'un consensus vers un autre [...] Et donc, pour moi l'évolution, si tu veux [...] la modification d'une blockchain, on part dans l'inconnu [,] dans des choses qui ne sont pas spécifiées » [N. Bacca ; Entretien n° 8]. Là où la procédure des PR est un dispositif que les *bitcoiners** empruntent à la production de logiciels libres et aux forges, celle des BIP est l'institutionnalisation d'un dispositif *ad hoc* permettant de spécifier cet indéfini originel, relatif à l'évolution des règles de consensus : dès 2011,

A. Taaki (rencontré dans le Chap. I) a proposé une procédure standardisée « *permettant de proposer de nouvelles fonctionnalités, de recueillir les commentaires de la communauté sur un problème et de documenter les décisions de conception prises pour Bitcoin* »⁴³³. Puisque modifier les codes du consensus *par le protocole* que tous les *bitcoiners** suivent volontairement représente une révolution politique, la procédure du BIP est plus exigeante que celle encadrant les modifications incrémentales. L’acceptation communautaire renvoie à « *un seuil très très différent* » [M. Corallo, Entretien n° 15]. Comparativement à la procédure simplifiée, la production du consensus sur une évolution touchant aux règles canoniques consensuelles doit être globale, entre toutes les parties prenantes du Bitcoin : soulignée par la présence de chaque groupe aux étapes successives de la procédure - les développeurs* (1), mais aussi les membres du groupe mineurs et assimilés (2), des utilisateurs finaux (3), des différents services marchands et de passerelles* (4), des médias et chercheurs (5). D'où des processus impliqués par la procédure des BIP « *très différents dans le sens où, vous savez que vous avez la liste de diffusion, le processus BIP, [...] en parallèle, vous devez développer le code, le faire examiner lourdement et évidemment, cela concerne plus que vous et l'équipe Bitcoin Core, vous avez aussi besoin d'avoir un certain niveau de compréhension de si la communauté est soit en faveur, soit contre un tel changement* » [M. Corallo ; *Ibid.*]. Un BIP doit fournir une « *spécification technique concise de la fonctionnalité et une justification de cette dernière* » et sert tout à la fois à « *proposer de nouvelles fonctionnalités, [à] recueillir les commentaires de la communauté sur un problème et [à] documenter les décisions de conception prises pour Bitcoin. [...] Les BIP étant conservés sous forme de fichiers texte dans un référentiel de versions, l'historique de leurs révisions constitue la trace historique de la proposition de fonctionnalité* », et c'est son auteur qui « *est responsable de la création d'un consensus au sein de la communauté et de la documentation des opinions divergentes* » (Taaki 2011).

Les BIP sont tout à la fois un outil de proposition et d’évaluation par les pairs, un support de débats et d’amendement et, finalement, un outil de documentation et de consignation permettant d’archiver de manière transparente les différentes décisions qui ont conduit aux codes de Bitcoin reconnus par la majorité. En tant que procédure formelle, elles déplacent les problèmes sur un champ procédural ordonné et permettent de limiter la survenue de conflits personnels, voire d’attaques *ad hominem* (les développeurs* peuvent y intervenir sous pseudonyme). Ce dispositif *off chain** est multifacette, relevant dans sa pratique d’une forme instituée de résolution de crises et conflits : à la formalité du BIP répond l’informalité de la « *création d'un consensus au sein de la communauté* », suivant une publicisation large au sein d’arènes de débats différenciées et de dispositifs hétérogènes permettant de mesurer l’assentiment général, *via* l’établissement de dispositifs variés à la fois *on chain* et *off chain**. L’étendue des changements proposés commande une publicité large. Mais si les BIP (comme les PR) sont publiés et soumis à relecture *via* le répertoire Bitcoin Core (utilisé par les techniciens), les discussions les entourant impliquent plus largement l’ensemble de la communauté. Les informations et débats, pour aller au-delà des groupes techniciens, se font par des canaux et arènes plus larges et inclusifs (« *Bitcointalk* », « *Crypto Twitter* », « *Reddit* », etc.). Les discussions « techniques » des arènes de développeurs* sont traduites par les médias et chercheurs (5), ainsi que par chacun des membres des différents groupes et factions, à travers les débats publics, les compagnes de communication, l’organisation d’évènements, la publication d’information et de prise de position (développeurs* (1), mineurs et assimilés (2), utilisateurs finaux (3), services marchands et de passerelles* (4)). Quant aux dispositifs de mesure du degré d’acceptation d’une modification, ils constituent une question épineuse. Comment évaluer l’accord ou le refus des membres de la communauté alors même qu’il est impossible d’identifier ces derniers exactement ? Si le consensus *par le protocole* repose sur la PoW*, qui permet de s’assurer de l’absence d’*attaque sybille**, il n’en

⁴³³ Le BIP 0001 original décrit l’objectif et les moyens de cette procédure. Voir <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki> [consultation au 05/12/2021].

est pas de même pour ce qui touche au consensus *sur* le protocole. En dehors de la chaîne*, rien ne permet de se prémunir contre le fait que des acteurs multiplient les comptes, pour donner à leurs propres avis l'apparence d'un consensus large (pratique dite d'« *astroturfing* » largement présente et documentée dans le champ des CM, voir Lielacher et Pickering 2020 ; Redman 2019). La mesure de l'assentiment communautaire a historiquement relevé de plusieurs dispositifs *ad hoc* s'adaptant aux situations et aux acteurs concernés : au sein de la chaîne *via* la mise en place de procédures de signalement et d'activation⁴³⁴ accessibles aux opérateurs de nœuds* mineurs, et aussi *via* des procédures *off chain** permettant de récolter l'avis des autres groupes de la communauté (cf. section III.3, dédiée à une crise « d'évolution » à gouvernance publique, qui sera l'occasion de traiter ce type de dispositifs).

Ainsi, les deux types de procédures d'évolution de Bitcoin assurent la production d'un consensus, mais leurs formes diffèrent. Là où un BIP impose de mobiliser l'ensemble des composantes communautaires de Bitcoin, la procédure simplifiée des PR, elle, déroge à ce principe de publicité large des débats et se satisfait d'un consensus essentiellement local entre spécialistes.

Gouvernance de huis clos : consensus local *ex ante* entre une poignée d'acteurs en réseau*

Comme nous l'avons vu, la faille Bitcoin CVE 2018 illustre une face importante de la gouvernance de Bitcoin : sa forme de huis clos. La procédure des PR, au cœur de l'activité quotidienne de maintenance infrastructurelle de Bitcoin et ouverte aux évolutions incrémentales, se satisfait d'un consensus local. Et toutes les modifications ayant concouru à cette crise, qui ont introduit les failles ou qui ont plus tard cherché à les corriger, relevaient de cette procédure et non des BIP (cf. Figure 13). L'étude de la crise Bitcoin CVE 2018 permet de retracer les canaux de communication mobilisés dans le cadre de la procédure simplifiée. Tous reflètent la publicisation faible, cantonnée à la communauté restreinte des « super utilisateurs » (Github, canal IRC ; Tableau 8 ci-après).

⁴³⁴ Ces procédures d'activation évoluent au gré des besoins et « les propositions de nouveaux mécanismes d'activation de Soft Forks sont souvent conçues pour éviter les problèmes rencontrés lors de Soft Forks précédents » (Optech 2021). Par exemple, la BIP 0009 mise en place en 2015 permet de définir un laps de temps (exprimé en nombre de blocs) après lequel une mise à jour sera enclenchée à condition qu'elle ait reçu le soutien de suffisamment de nœuds*. La temporalité comme le quorum devant être définis dans la proposition BIP. Voir <https://github.com/bitcoin/bips/blob/master/bip-0009.mediawiki> [consultation au 06/12/2021]. D'autres procédures de ce type seront implémentées comme pour le BIP 0034, le BIP 0066 ou le BIP 0065, Optech (2021) qui fournit un aperçu des procédures d'activation historiquement notables.

Tableau 8 : Les différents canaux d'information et de discussion mobilisés lors de la crise CVE 2018

Type de canal d'information mobilisé	Canaux informationnels dégagés lors de notre enquête	Caractéristiques
Canal de sécurité Bitcoin Core	« Page contact Bitcoin Core ⁴³⁵ » : transmission du rapport de divulgation responsable à P. Wuille, G. Maxwell & W. Van der Laan, de l'équipe Bitcoin Core (Bitcoin Core 2018a; Awemany 2018)	Canal de sécurité formel et privé indiquant les acteurs à contacter (adresse mail et clef PGP).
Canaux privés divers	P. Wuille transmet le rapport à C. Fields, S. Daftuar, A. Marcos et M. Corallo (Bitcoin Core 2018a). M. Corallo le trouve sur son bureau à « Chaincode labs » et en discute avec ses collègues Marcos et Daftuar [Entretien n° 20]	Canaux d'information informels et privés permettant la coordination des acteurs participant à la remise en ordre (importance du capital culturel des acteurs comme de leur capital social)
	Prise de contact téléphonique entre M. Corallo et les CEO et CTO de la <i>pool</i> de minage « Slush pool » ; J. Newbery et J. O'Beirne sont informés par M. Corallo de la faille et contactent « différentes entreprises du secteur » (<i>Ibid.</i>)	
	N. Bacca reconnaît avoir connaissance d'un problème par une connaissance avant même la divulgation publique [N. Bacca, Entretien n° 8]	
	Les échanges sur le canal IRC du 18 septembre 2018 démontrent que Luke Dashjr a connaissance du bogue et qu'il est en charge de signaler la vulnérabilité à l'autorité d'identification CVE (voir ci-après)	
Canaux publics divers	Répertoire « Bitcoin Core » sur « Github »: échange concernant la faille et les correctifs (<i>Ibid.</i> ; Awemany 2018)	Canaux d'information formels et informels majoritairement publics permettant une publicisation large en direction de l'ensemble de la communauté
	Canal IRC #bitcoin-core-dev (freenode, 18/09) : Luke Dashjr, qui n'apparaît pas dans la divulgation complète, écrit sans plus de précision : « Pour ce que ça vaut, j'ai obtenu le CVE 2018 17144 pour cela »	
	Publication de la divulgation complète par « Bitcoin Core » sur le site Bitcoin Core (Bitcoin Core 2018)	
	Publication d'informations : billet de blog, podcast/vidéo, etc. (Song 2018 ; Awemany 2018 ; Bitcoin Q&A 2018 ; jnewberry-cve-2018-17144-bug ; Straw Hat 2019)	

Source : Rolland Maël

La publicisation du bogue CVE 2018 ne fut ni totale, ni réalisée d'un seul coup, ni directement à l'adresse de la communauté dans son ensemble. Pendant les phases d'évaluation du problème et de développement/test de solutions correctives et jusqu'à la publication du rapport de divulgation complète par l'équipe Bitcoin Core, le bogue de « faux monnayage » est dissimulé et seule la faille DOS est publique (Bitcoin Core 2018 ; Entretien n° 15). Cette logique de rétention/libération graduelle de l'information renseigne sur les liens existant entre les acteurs impliqués. Les informations furent d'abord partielles et tournées vers des réseaux* d'acteurs ayant la confiance des développeurs* Bitcoin Core. Ce n'est que durant la phase de résolution, à la suite du dépôt public des correctifs sur GitHub, puis par la publication du rapport de divulgation complète, qu'un

⁴³⁵ <https://bitcoincore.org/en/contact/> [consultation au 08/12/2021].

consensus global entre tous les *bitcoiners** a pu se former, via la mobilisation de canaux publics et non plus privés.

Dans le cadre de cette gouvernance de huis clos, la phase d'évaluation n'a impliqué qu'une poignée d'acteurs en réseau* aux liens forts. Sur le « repo Bitcoin Core », l'enquête fait ressortir que le nombre de contributeurs, bien qu'en augmentation, reste relativement restreint et cantonné au même groupe d'intervenants en ce qui concerne les activités critiques (moins d'une vingtaine d'acteurs impliqués dans les PR recensées). Nos entretiens avec des acteurs aux compétences techniques reconnues sur Bitcoin, au sein de la communauté parisienne [Anon 1, 2, 3 et 4] ou plus globalement dans la communauté Bitcoin élargie [J. Song, M. Corallo, A. Le Calvez] démontrent que, bien que formellement ouvertes à tous, ces activités ne sont accessibles qu'à certains : à l'exception de Corallo et Song, tous les acteurs rencontrés se déclarant codeurs Bitcoin reconnaissent n'avoir jamais réalisé d'activité de code, voire de relecture, car ils « *ne maîtrisent pas* » suffisamment le langage de programmation* de Bitcoin Core (cf. le C++, Chap. I) : « *je le lis comme ça, je peux comprendre ce que ça fait mais de là à review vraiment...* » [S. Roche ; Entretien n°23 ; idem pour Anon 1, 2, 3, 4 et L. Thiébaut]. Au-delà des statuts formels dégagés entre « Core Devs » (cf. Core mainteneur et développeur* simple), d'autres plus informels existent suivant les activités et compétences impliquées. Au sommet, les plus compétents participent de la catégorie des « chercheurs », car « *des idées, par exemple Segwit, il faut bien avoir quelqu'un qui a eu l'idée et qui la vendre aux autres* » [A. Le Calvez, Entretien n° 20]. Song s'exclut de cette catégorie, car tout le monde n'est pas en capacité de « *dire "oui, nous devrions faire ceci ou cela"* [...] , d'avoir assez d'influence pour pouvoir le faire,[et] la plupart des personnes qui parlent de ces choses sont impliquées depuis plusieurs années. » Lui se voit, avoir le « *rôle [d']un éducateur [:] je prends ce qu'ils disent et puis j'interprète pour les gens qui ne comprennent pas vraiment. [...] Je suis plus un enseignant qu'un chercheur* » [J. Song ; Entretien n° 17]. Ces chercheurs à la P. Wuille (à qui l'on doit la BIP SegWit) sont les « super codeurs » qui ont la confiance des *bitcoiners**⁴³⁶. Cette confiance n'est jamais donnée, il faut des membres, comme Song, plus nombreux à la base, pour assurer relecture, traduction et vulgarisation. D'ailleurs, ce cadre procédural ordinaire évolue et s'intentionnalise afin d'assurer qu'un travail minimum sur chaque PR soit réalisé : la relecture par les pairs est ainsi passée de l'informalité des contributions volontaires à un dispositif d'assignation formel de relecteurs (ce qui apparaît pour les PR #9049, #10195 et #10537, Figure 9 précédente ; rapporté aussi par S. Roche ; Entretien n° 23].

Corallo [Entretien n°15] fait aussi partie des chercheurs peu nombreux, comme ses collègues de bureau avec qui il partagea la découverte du rapport de divulgation responsable. Et seuls ces chercheurs arrivent, tant bien que mal, à se faire financer. Le financement des personnes en charge de la maintenance et de la sécurité de la couche protocolaire de Bitcoin est « *un problème [...] intéressant [...] à regarder* » : malgré la valeur générée, il n'y a finalement que « *très peu de gens en fait, dans les boîtes autour de l'écosystème, qui sont impliqués dans les couches protocolaires, en tout cas sur Bitcoin [:] Ethereum c'est un peu l'exception avec Consensys [et] la fondation Ethereum [en comparaison] Blockstream [...] c'est ce qui pourrait se rapprocher le plus [...] d'un truc comme l'Ethereum Foundation dans le monde de Bitcoin* » [N. Bacca, Entretien n° 8, rejoint par Léa Thiebaut, Entretien n° 21]. Rapporté à d'autres projets à codes sources ouverts, ce problème structurel s'expliquerait par l'absence d'*« une culture qui va fonctionner un petit peu comme tu peux avoir sur Linux aujourd'hui. Les choses s'y sont extrêmement professionnalisées et au final tu as toutes les grandes distributions qui participent aussi au noyau. Tu n'as pas du tout cette équivalence en fait aujourd'hui dans les cryptomonnaies**. Donc tu as extrêmement peu [...] de développeurs*

⁴³⁶ « In Super Coders We Trust », voir <https://twitter.com/APompliano/status/1420095187578195974?s=20> [consultation au 01/01/2022].

Bitcoin sur le... au niveau du protocole et du consensus qui sont dans une boîte. » [N. Bacca, Entretien n° 8]. À l'exception de l'entreprise de Corallo et ses collègues, « ChainCode labs », ou encore de « Blockstream », explicitement tournées vers la recherche et le développement de Bitcoin qui leur offrent des contrats de travail en vue de financer leurs travaux sur Bitcoin Core⁴³⁷ (BitMEX Research 2020a), bien peu nombreux sont les développeurs* Bitcoin à pouvoir en vivre [Stéphane Roche, Entretien n° 23].

Justement, le contact que Corallo ouvre avec Slush Pool relève de ces liens forts entre les personnes et les organisations dont elles sont membres : Slush Pool développe le protocole de minage Stratum V2 sur une idée originale de Corallo de ChainCode Labs (Wirdum 2019). De fait, de ces liens existants, « *Slush Pool est beaucoup plus facile et plus fiable à contacter, que beaucoup de... pools chinois [, à cela s'ajoute] aussi le fuseau horaire, c'était... un fuseau horaire raisonnable pour l'Europe, ce n'était pas un fuseau horaire raisonnable pour la Chine.* » [M. Corallo, Entretien n° 15]. Si les codeurs se font législateurs, l'application de la loi nécessite les mineurs, d'où ce contact privilégié avec une pool amie, où ils sont invités à participer aux débats privés en qualité d'experts de confiance.

Ainsi, c'est au cours d'une discussion confinée qu'un premier consensus *ex ante* sur la validité et la légitimité des correctifs s'est construit au sein d'un collège restreint d'acteurs et en dehors des canaux d'information publique. La production et la mesure du consensus entourant ces modifications se sont limitées à l'absence d'opposition frontale des participants, sachant que, dans le cadre de cette procédure, les conflits sont rares, voire inexistant⁴³⁸. D'où des PR fusionnées dans la branche principale du répertoire pour être implémentées dans une nouvelle version logicielle : ces changements sont « *rapidement considéré[s] comme bon[s] dans l'examen par les pairs, ACKed dans le langage du Core* » (Awemany 2018). Mais cela n'est pas suffisant ! Encore faut-il qu'un consensus communautaire large soit réalisé *ex post*, alors même que lesdits correctifs touchent aux règles canoniques consensuelles de Bitcoin.

Unanime et inaperçu : l'Audience Publique sans vague d'une crise et sa résolution

La crise Bitcoin CVE 2018 n'est ni la plus controversée, ni la plus politique, donc - en théorie - pas la plus intéressante au sens de Callon (2006). Cet auteur a montré l'importance des controverses et conflits, comme « *épicentre* » et « *point de fusion* » où la « *technique prend forme* »,

⁴³⁷ « *C'est tous des gens qui sont de leur côté, qui font des trucs, tu peux en avoir quelques-uns chez Blockstream mais c'est... et même, enfin je veux dire, Blockstream aujourd'hui je considère que c'est plus une boîte de recherche, tu vois* » [N. Bacca, Entretien n° 8]. Blockstream faisait partie des sponsors des événements « Breaking Bitcoin » (Observation participante n° 14 et 25, Annexe n° IV.2), dont l'une des organisatrices nous apprend que « Chaincode Lab » organise aussi des formations « *sur plusieurs semaines de “relecture” (“review”) autour de la proposition de modification “Taproot”. [...] Organisé par des core dev [...] Et en fait c'était sur 7 semaines normalement, c'était quatre fois par semaine, 40 heures par semaine. J'ai arrêté parce que c'était trop... trop chronophage, j'étais un petit peu larguée et en fait c'était une review avec toutes les semaines un sujet différent sur un petit peu de tout : “Taproot”, “Grassroot”, “Schnorr”, “MAST” [...]. On était 160 au début, je crois que ça a terminé avec beaucoup moins [...]. J'étais déjà extrêmement contente que leurs initiatives au groupe 160 personnes, j'ai trouvé que c'était vraiment génial, ils ont organisé ça mais de manière incroyable, les mails, les machins... on sentait vraiment qu'il y avait un énorme investissement de la part des organisateurs pour faire en sorte de rendre le travail fluide pour tout le monde* ».

⁴³⁸ Questionné sur l'apparition de conflits entre développeurs* suite à de simples PR ou à des BIP, M. Corallo nous répond : « *Vraiment pas... Vous savez, en général il y a très très peu de conflits, voire aucun. Vous savez, évidemment il y a beaucoup de discussions couvrant les changements [/] il y a des demandes de Pool Request et les gens ont beaucoup à dire sur les choses mais [...] ce n'est jamais vraiment litigieux [...]. En général, relativement, très peu de conflits dans ce domaine. [...] Quand vous regardez les changements du système de consensus et que toute la communauté doit être d'accord, il y a eu des conflits, mais en termes de changements du logiciel de base de bitcoin, il n'y en a vraiment pas beaucoup.* » [M. Corallo, Entretien n° 15]

mais s'il reconnaissait que les controverses « *ne manquent pas* », pouvant « *surgir de partout* », leur choix nécessiterait une attention particulière (*Ibid.*, p. 2-3). Se libérer « *d'un monde préconstruit* » impose de trouver des controverses « *suffisamment ouverte[s] dans l'[es]quelle[s] les négociations sont multiples, la nature des choix est encore discutable, les acteurs impliqués nombreux et variés, les exclusions non définitives* » (Callon 2006, p. 4). Une « bonne » controverse se définit par quatre caractéristiques (*Ibid.*, p. 5) comme pour celles entourant les véhicules électriques légers (VEL) : la controverse portait bien « *sur un objet technique [...] non réductible à de la pure technique* », car différents types d'argumentaires (scientifique, économique, etc.) disputent continuellement les arguments techniques ; « *les solutions envisagées étaient bien multiples* » et renvoient à des problématiques différentes suivant les acteurs, « *les groupes sociaux impliqués et leurs intérêts [y étaient] aussi nombreux et variés que possible* », ce qui conduit certains acteurs à privilégier certaines problématiques au détriment d'autres. Enfin, « *les forces qui s'opposent [...] s'équilibrivent en permanence* », ce qui « *rend peu efficaces les arguments d'autorités [,] permet à la controverse de demeurer ouverte* ». Et si certains acteurs parviennent à faire triompher leur voix (et à faire taire celles des autres), celle-ci peut-être bien « *vite contesté[e] et débordé[e] de tous côtés* » (*Ibid.*, p. 5). Sur ces critères, seul le premier est activé dans notre cas. Bitcoin est un objet socio-technique et ses règles canoniques consensuelles, ainsi que les discussions entourant leurs définitions/modifications, ne se réduisent pas à de simples problématiques techniques : le monnayage, comme les règles encadrant les transactions* – vérification et sanction des doubles dépenses – relève bien de justifications et de négociations hybrideant des argumentaires économiques, techniques, philosophiques. De ce fait, cette crise apparaît plus comme une crise « *post-technologique* » où Bitcoin est déjà « *réifié* » en bonne partie (*Ibid.*, p. 4)

Si l'absence de débats et controverses durant la crise peut s'expliquer par la confidentialité de la remise en ordre, la persistance de cette absence après la divulgation complète éclaire la question de la nécessité d'un consensus communautaire *a posteriori*. Il s'y joue la reconnaissance de la légitimité des actions secrètes et discrétionnaires, construite dans l'épreuve. Nous en voulons pour preuve le bouleversement explicite des représentations de certains *bitcoiners** suite à cette crise : « *au début, j'étais de ce côté-là* [de l'interprétation rigoriste du « *Code is Law* » à la Szabo, NDA]. *En effet, ben si le code dit cela, il va se passer cela. J'étais encore de ce côté-là pendant la "CVE 2018 je ne sais plus quoi là" ... je me suis dit, ben finalement si quelqu'un avait exploité cela, est-ce qu'il aurait fallu accepter ou pas les changements ? Je me suis dit bon... il a fait ça, ok... Pareil avec "The DAO", avec le temps je me dis qu'il y a quand même un consensus social. "Code is law as long as people don't mind"* » [A. Le Calvez, Entretien n°20]. Cette citation montre l'évolution et la formation d'un consensus sur le fait que la lettre du code ne peut à elle seule prétendre à être « *loi* » : la déférence au code et la légitimité des interactions réalisées au sein de la chaîne renvoient d'abord à des interprétations humaines.

D'un côté, les versions logicielles vulnérables publiées (et celles implémentant les correctifs) peuvent être conçues comme des évolutions radicales de type *Fork**, car elles touchent aux règles consensuelles canoniques pour tout *bitcoiner* (Hacker News Forum et Apo 2018, rejoint par Awemany 2018). Du côté des *bitcoiners**, ces changements non anticipés n'ont pas été consciemment implémentés, d'où la qualification en termes de vulnérabilité. En tant que crise « *de vulnérabilité* », la déviance est explicite pour les *bitcoiners**, les codes vulnérables permettant des actions considérées *a priori* comme illégitimes. Personne, de Nakamoto aux autres *bitcoiners**, n'a imaginé que le faux monnayage et la double dépense puissent être légitimes. Aucun doute chez les acteurs : les comportements de double dépense permis par les versions 0.15.x-0.16.x, comme le faux monnayage induit, ne relèvent ni de la lettre du code acceptée (les règles contenues et rendues exécutoires par les versions précédentes), ni de son esprit. D'où un consensus sous la forme d'une absence de dissensus, exprimée à la fois par la mise à jour rapide vers les versions corrigées par les

opérateurs de nœuds* vulnérables et l'absence notable de débats et conflit intracommunautaire entourant cette crise et sa révélation publique finale. Au cœur de la résolution de cette crise, pas de controverse technologique, au sens de Callon (2006, p. 5) : *les solutions envisagées* ne furent pas *multiples* et la remise en ordre peu complexe. Il a suffi de réintégrer les vérifications de validité qui avaient été supprimées, car considérées à tort comme redondantes. En outre, *les groupes sociaux impliqués et leurs intérêts* n'y étaient pas *nombreux et variés*. Enfin, difficile d'y voir un *équilibre de force* en opposition permanente : ni la mise en crise, ni la remise en ordre n'ont conduit à des controverses à l'intérieur de la communauté Bitcoin. Les critiques extra-communautaires sur la gravité et la gestion irresponsable des « Core Devs » proviennent principalement de ceux qui ont subi la défaite du « Scaling Debate », les membres de la communauté « Bitcoin Cash », et apparaît une tentative de réactiver la controverse : « *600 microsecondes* », c'est « *le temps que Matt Corallo voulait rogner sur la validation* des blocs avec sa Pull Request de 2016 sur Bitcoin Core* » alors que, à l'époque, d'autres solutions proposées par les *Big Blockers* permettaient des gains de propagation plus importants (Awemany 2018). Néanmoins, pour les *bitcoiners**, ces questions sont closes, les critiques exprimées ne visent qu'à « *gonfler hors de [leurs] proportions* » les conséquences de cette crise afin de « *faire paraître ce bug pire pour que [Bitcoin Cash] ait l'air meilleur* » (McCormack et Song 2018). Suite à la divulgation complète, la communauté Bitcoin reconnaît sa gravité potentielle, mais ne le fait qu'en soulignant sa faible gravité réelle (Song 2018, Antonopoulos 2018) et en se félicitant des conditions dans lesquelles les « Core Devs » ont rapidement conduit la remise en ordre : « *ce qu'il faut regarder, c'est la gravité des bogues (celui-ci était grave), la rapidité avec laquelle ils sont corrigés, s'ils sont exploités avant d'être corrigés ; s'ils le sont, quelles sont les conséquences à long terme et s'ils ont un impact durable. [...] Les systèmes [de réponse] sont [déployés] lorsque les choses tournent mal, et le système continue de fonctionner. [Ce bug] n'a pas tué Bitcoin, il l'a rendu plus fort, ce qui est l'un des aspects de Bitcoin qui... continue de me surprendre, dans sa résilience* » (Antonopoulos 2018). Cette crise Bitcoin CVE 2018, en tant que crise « de vulnérabilité » à gouvernance de « huis clos », présente l'intérêt d'éclairer la « micropolitique » qui est au cœur de la maintenance des codes de Bitcoin. Elle permet de décenter l'analyse vers les activités quotidiennes de maintenance, qui, du point de vue des acteurs, paraissent moins critiques, et relèvent d'une gouvernance routinière et normalisée.

L'absence de dimension vraiment critique, politique et conflictuelle de la crise Bitcoin CVE 2018 se mesure à l'aune de sa faible connaissance dans la communauté des *coiners**. Cette crise est loin d'avoir donné lieu à la même quantité d'analyses et de commentaires que les « crises d'évolution », dont le « Scaling Debate » est emblématique (cf. Chap. II, section II.3.3). La crise est une affaire de visible et d'invisible, plus exactement de visibilisation et d'invisibilisation. L'histoire des crises « de vulnérabilité » *aconflictuelle* de Bitcoin (cf. Chronologie 4) est donc en général mal connue des membres de la communauté. Les *bitcoiners** rencontrés méconnaissent aussi bien la dénomination de la faille que ses caractéristiques et enjeux, son déroulé et les conditions de sa résolution. À la question type de savoir quand et comment nos intervenants ont eu connaissance de cette faille, les réponses révèlent que ce « *CVE 2018 je ne sais plus quoi* » [A. Lecalvez, Entretien n° 20] a laissé peu de traces dans la mémoire des *bitcoiners**. S. Gouspillou [Entretien n° 17], n'ayant aucune connaissance de cet événement, nous redirigera vers Jean-François Augusti, le CTO de son entreprise ayant à charge ce type de problématique technique. Ce dernier nous répond : « *Houla, pas du tout [...] ben écoute, non, non, non, je regarde en même temps que tu m'en parles. J'en ai peut-être entendu parler alors, mais cela ne m'a pas du tout... j'ai pas du tout percuté.* » [J.-F. Augusti, Entretien n° 18]. Même connaissance imprécise de la part de M. Phuc : « *alors attends, qu'est-ce qui s'est passé ? Rafraîchis-moi la mémoire.* » [...] « *Ça, je me souviens, c'est assez marrant parce que... [...] tu vois, tu as dû me le remémorer. Mais je me souviens que cela ne m'avait pas beaucoup marqué [...], bon même si on avait traité évidemment le sujet [dans le Journal du Coin, NDLR].* » [Entretien n° 19]. S. Roche abonde : lui aussi a « *dû vérifier lequel c'était [...]* »,

tout en reconnaissant n'avoir pas vraiment « creusé » la question bien qu'il en ait pris connaissance à l'époque : « *Ouais [...] j'ai lu l'annonce pour comprendre de quoi il s'agissait.* » [Entretien n° 23]. L. Thiébaut, elle non plus, n'est « *pas sûre de l'avoir vu passer celle-là* » et d'ajouter : « *si tu veux, j'en ai pas entendu parler de cette faille parce que j'ai l'impression qu'elle n'a pas fait trop parler d'elle...* ». En même temps, elle nous « *avoue, [que] les CVE [, elle] ne les suit pas trop, parce que [...] une fois que c'est publié, c'est trop tard pour que cela soit marrant [elle rigole un peu]* » [L. Thiébaut, Entretien n° 21].

La crise Bitcoin CVE 2018 « *n'a pas fait trop parler d'elle* » [*Ibid.*], car, par construction, les crises « de vulnérabilité » n'impliquent pas de dissensus communautaire. Dans le cas contraire, la gouvernance de huis clos dégagée se transforme en gouvernance ouverte et publique. L'histoire des crises Bitcoin présentée dans la Chronologie 4 le montre : certaines mises en crise ou remises en ordre passent par la procédure des BIP (différenciée des PR dédiées à la maintenance) et peuvent être moins consensuelles, comme l'illustre, pour Bitcoin, le « Scaling Debate » ou l'épisode du HF d'Ethereum consécutif à l'attaque de « The Dao », que nous allons étudier à présent.

III.3 UNE GOUVERNANCE PUBLIQUE D'EXCEPTION : LE *HARD FORK* D'ETHEREUM CONSÉCUTIF À L'ATTAQUE DE « THE DAO »

Jusqu'à présent, notre enquête au cœur des crises protocolaires de Bitcoin a pointé l'existence d'une gouvernance de crise à double face, qui va avec la définition d'une nomenclature de « pathologies » mais aussi d'acteurs, de lieux, canaux, procédures et dispositifs d'interactions, de contention et de remédiation. À l'image de son développement, la gouvernance de Bitcoin et des CM est également carnavalesque. Elle se fait théâtre où se jouent des drames complexes, mêlant secrets bien gardés et débats publics enflammés. La crise Bitcoin CVE 2018 a principalement attiré l'attention sur la gouvernance de huis clos - les coulisses - que nous avons pu documenter et analyser. Cette face routinière de la gouvernance *sur le protocole et la centralité*, qui prend le groupe restreint des « Core Devs », a déjà été saisie et analysée par d'autres auteurs qui concluent à une gouvernance fondée sur « *une structure de pouvoir hautement technocratique* », sise sur une logique « *autocratique-mécanique* » avec « *des élites excessivement centralisées* » autour d'un « *dictateur philosophe* » (De Filippi et Loveluck 2016, p. 12-13 ; cf. Chap. II section I.3.3). L'analyse de la gouvernance *sur l'infrastructure d'une CM* ne peut s'arrêter à cette face. La gouvernance de huis clos est toujours suspendue à l'absence de dissensus communautaire, dont la gouvernance ouverte et publique est le contrepoint nécessaire, qu'il nous reste à analyser.

Des acteurs ont ainsi critiqué des analyses qu'ils considèrent comme partielles⁴³⁹, voyant dans cette vision d'une administration des codes Bitcoin comme « *point de contrôle unique [,] un faux-fuyant qui découle d'une perspective autoritaire* » (Lopp 2018). À ces critiques, les *bitcoiners** répondent qu'une épée de Damoclès pèse sur toute tentative d'imposition discrétionnaire de code que la communauté jugerait contraire à ses intérêts : la « *liberté de l'open source* » offre à « *quiconque est insatisfait du projet Bitcoin Core* » ou « *en désaccord avec les "mainteneurs"* », la liberté de lancer le sien en propre, en partant de zéro ou en « *Fork*ant* » les codes existants. L'administration du répertoire « *Bitcoin Core* », en tant qu'il est un système de ressources (Hess et Ostrom 2007) essentiel de la gouvernance *sur l'infrastructure*, serait substituable par d'autres, qui

⁴³⁹ Lors de notre enquête de terrain et de nos entretiens, plusieurs acteurs nous ont fait part rapidement de l'avis négatif qu'ils pouvaient avoir sur des travaux académiques traitant de Bitcoin et des CM, en citant particulièrement ces travaux. Cf. Introduction générale, section C. 1 et note 46.

pourraient assurer des fonctions similaires : le travail des développeurs* (et les productions/unités de ressources qui en résultent, peuvent être déplacées vers « *un dépôt différent sur lequel les mainteneurs de Bitcoin Core n'auraient aucun privilège administratif* » (*Ibid.*). C'est cette possibilité toujours ouverte aux *bitcoiners** de s'opposer à des modifications non consensuelles par le *Fork**, qui leur garantirait en dernier ressort de conserver la souveraineté du choix des règles canoniques consensuelles qu'ils suivent. Si notre propre travail souligne la structure technocratique du sous-système de ressources qu'est le répertoire Bitcoin Core, impossible d'en tirer des conclusions. Encore faut-il éprouver l'affirmation que les « Core développeurs* » disposent plus d'une « *fonction de concierge [que d']un poste de pouvoir* » (*Ibid.*), ce qui nécessite de voir en action l'ensemble des règles et dispositifs précédents qui visent à le garantir. Faire ce travail était difficile pour De Filippi et Loveluck (2016) : analysant un « Scaling Debate » encore en phase d'insémination, ils n'avaient pas accès aux matériaux de la remise en ordre sous forme de schisme de 2017. Ces matériaux ont étayé l'idée que les pouvoirs étaient concentrés dans l'espace des priviléges/faisceaux de droits que les mainteneurs ont sur le répertoire « Bitcoin Core » et que ces derniers se muent en autorité, que peuvent reconnaître ou refuser les acteurs des autres sous-systèmes imbriqués participant de la gouvernance *sur* l'infrastructure Bitcoin. Routinièrement, la reconnaissance de cette autorité se fait tacitement et sans ambages, comme avec le cas Bitcoin CVE 2018. La situation diffère avec les crises « d'évolution » qui conduisent inéluctablement à des débats, voire des conflits, eux, résolus sur une « grande scène » *via* une gouvernance publique. C'est lors de l'expression rare et intermittente de cette seconde face de gouvernance que les acteurs des autres sous-systèmes de ressources (minage, services marchands et passerelles*, utilisateurs finaux, médias et chercheurs) se parent des costumes du contre-pouvoir, et que l'ensemble des mécanismes communautaires de contrôle visant à assurer la production de consensus (et d'expression du dissensus) est mobilisé (comme la procédure des BIP, décomposée dans la Figure 12 précédente, l'illustre).

La crise du « Scaling Debate », építome d'une controverse technologique à la Callon (2006, p. 5, cf. Encadré n°4 Chap. II, section II.3.3) est emblématique de l'ontologie politique de Bitcoin : son dénouement par schisme protocolaire et communautaire a révélé les tensions en valeurs, ainsi que des attentes monétaires hétérogènes au sein de sa communauté. Mais Bitcoin, pour une fois, ne fut pas pionnier avec cette crise à gouvernance *publique*. C'est Ethereum qui a été le premier champ de bataille de ce type de guerre communautaire et protocolaire, avec le *Hard Fork** consécutif à l'attaque de « The DAO ». Ces deux crises partagent le fait de revêtir les caractéristiques d'une controverse technologique et un dénouement sous forme de schisme/*Fork** à la suite d'un conflit entre des visions antinomiques de ce que doit être l'objet monétaire, donc concernant les modifications de code désirables. Une première section reviendra sur les conditions brutales, publiques et tapageuses de la mise en crise. Puis, nous analyserons les conditions complexes, contraintes et controversées de la remise en ordre. Outre les enjeux débattus de la crise et ses conséquences, ainsi que des voies de remédiation souhaitables, nous ferons ressortir les grands traits de la gouvernance *publique* mobilisés durant cette crise. Nous reviendrons enfin sur la remise en ordre, qui produira un schisme protocolaire et communautaire surprise démontrant que, pour ces communautés de paiement, les *Forks* sont des moyens de retrouver, par sécession monétaire, le semblant d'homogénéité en valeurs que la crise avait fait voler en éclat.

III.3.1 Une mise en crise brutale, publique et tapageuse

Au-delà de sa proximité avec la crise du « Scaling Debate », ce sont ses différences qui nous conduisent à choisir la crise du *Hard Fork** d'Ethereum consécutive à l'attaque de « The DAO » comme deuxième terrain d'enquête. Tout d'abord, de 2015 à 2017, nous avions été témoin de nombreuses crises, de différentes importances, ayant touché l'écosystème des CM, dont les débats

et conflits consécutifs à ce problème de *débit** de Bitcoin. Nos premières réflexions sur la gouvernance de l'infrastructure Bitcoin (Rolland et Slim, 2017) puisent leur origine dans la controverse du « Scaling Debate ». Nous marchions dans les pas des travaux de De Filippi et Loveluck (2016), tout en souhaitant les actualiser et les préciser. Nous avions aussi découvert Ethereum peu après son lancement et participé aux premières ICO associées, dont celle très médiatique de « The DAO ». « The Dao » est un fonds d'investissement distribué sous forme de *smart contract**, dont un attaquant réussit à dérober une bonne part de la trésorerie. Cette situation conduit la communauté à se déchirer sur l'opportunité d'y remédier par un *Hard Fork**, une intervention discrétionnaire sur le protocole décriée chez les *coiners**. Ensuite, la crise d'Ethereum, en tant que pionnière, fait précédent et s'érite comme fondatrice : elle a participé à « créer l'Ethereum tel qu'il est aujourd'hui [et] une grande partie de la crypto telle que nous la connaissons aujourd'hui n'existerait pas » sans elle (Morris 2023 ; ce que souligne aussi V. Zamfir, Entretien n°9). Elle apparaît « *a posteriori* [comme] un moment historique qui aura des implications, très lointaines dans l'histoire de la création des concepts dans le numérique » [A. Roussel, Entretien n°11]. Le dénouement même du « Scaling Debate » n'est compréhensible qu'à la lueur de ce précédent dont les *bitcoiners** sont imprégnés (ce qui explique d'ailleurs pourquoi ils sont aussi nombreux à avoir un avis critique sur cette crise et sa gestion). La crise de « The DAO » est au cœur de la controverse entre *bitcoiners** et *etheristes* sur les questions de gouvernance de CM. Pour les premiers, la gouvernance d'Ethereum y apparaît frappée du sceau infamant de la centralisation et de la discréption, autour du fondateur Buterin et de la Fondation Ethereum. Notre choix d'étudier la crise « The DAO » provient aussi d'un accès au terrain facilité. À l'opposé d'un « Scaling Debate » trop vaste par le nombre de participants, ou de solutions proposées et dispersées dans sa temporalité, cette crise était plus accessible, car circonscrite, et nous y avions pris part en tant qu'usager (voir Immersions participantes, Annexe n°IV.1.). La singularité de cette crise apparaîtra dans la présentation de sa périodisation que nous allons aborder.

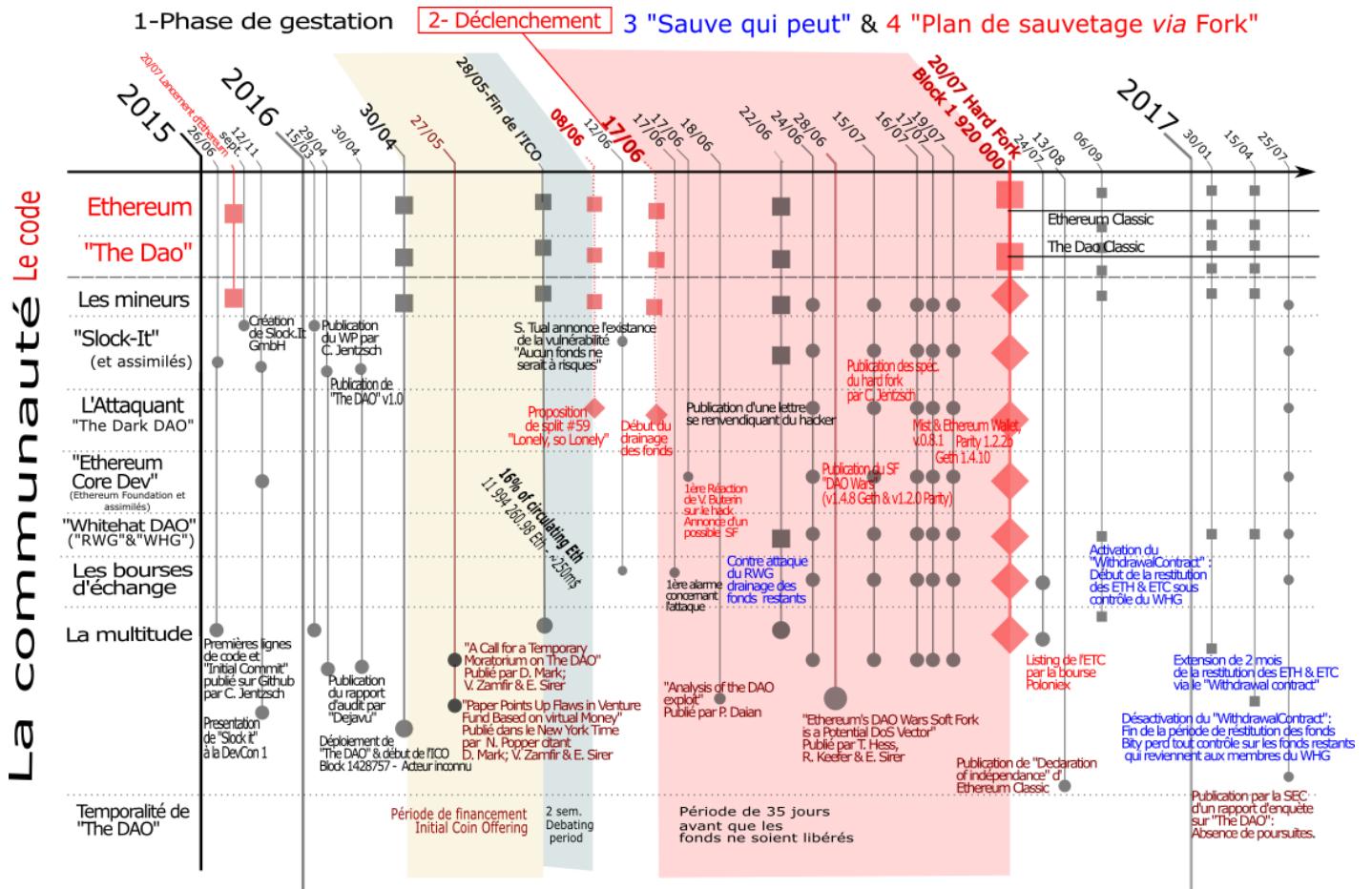
Périodisation du *Hard Fork** de « The DAO »

Ce cas d'étude, comme le précédent, permet d'interroger le rapport qu'entretiennent les *coiners** à l'« *autorité algorithmique* » (Lustig et Nardi 2015) et leur degré de « *déférence aux codes* » (Hinkes, 2021). Mais il apparaîtra plus crûment encore que les *coiners** peuvent mobiliser la gouvernance sur l'infrastructure pour amender la gouvernance *par* l'infrastructure de leur CM, afin de la faire coïncider aux attentes monétaires et politiques mouvantes qui traversent leur communauté. Les deux cas que nous avons choisis pour cette thèse offrent de forts contrastes, tant en termes de mise en crise que de remise en ordre. La crise du *Hard Fork** consécutive à l'attaque de « The DAO » revêt la forme d'une double crise emboîtée. Le point de départ est une crise « de vulnérabilité » liée à l'exploitation effective d'une vulnérabilité connue, « *terrible* » et « *largement répandue* » (Vessenes 2016a) concernant un fonds d'investissement distribué déployé sur Ethereum (sous forme d'une application en *smart contract**): il s'agit d'une faille dite de « *réentrance* (ou « *reentrancy* »/« *re-entry* ») qui permet à un « *attaquant* » de quitter le fonds en récupérant plus de capital qu'initialement investi (Atzei, Bartoletti et Cimoli 2017, p. 172 & 177 ; DuPont 2018, p. 6). Cette faille permet de « *demandeer de l'argent plusieurs fois avant que son solde ne soit mis à jour et que l'ordinateur ne s'aperçoive qu'il n'y a plus d'argent sur son compte* » (Russo 2020, p. 185). Cette crise « de vulnérabilité » touche d'abord la couche applicative, avant de muter en une crise « d'évolution », du fait d'une proposition de remédiation sous forme de modification des règles protocolaires canoniques. Là réside l'intérêt de cette crise : la résolution d'un problème circonscrit concernant un projet lancé sur Ethereum va passer par une modification du protocole Ethereum

lui-même⁴⁴⁰. Cette évolution, nous le verrons, s'explique par la jeunesse de cette CM qui, à l'époque, est encore en phase de « preuve de concept », d'où la centralité – réelle ou perçue - de V. Buterin et des membres de la Fondation Ethereum dans sa gestion. Les *bitcoiners** critiques de la gouvernance des événements ne doivent pas oublier comment Nakamoto fut central dans les crises – « de vulnérabilité » et /ou « d'évolution » – qui ont touché Bitcoin lorsqu'il était le seul mainteneur principal et que la crise Bitcoin CVE 2018 traitée précédemment, elle, est arrivée en phase de maturation de son développement infrastructurel (cf. Chap. I).

L'analyse de cette crise repose, comme nous l'avons fait pour la crise Bitcoin CVE 2018, sur une périodisation documentant les acteurs (humains ou non) et la structure de leur relation, à chaque étape de la mise en crise et de la remise en ordre (Chronologie 6 suivante).

Chronologie 6 : Périodisation de la crise consécutive à l'attaque de « The Dao »



Source : Rolland Maël

⁴⁴⁰ Ce qui explique pourquoi certains acteurs filent l'analogie (péjorativement) de l'action de prêt en dernier ressort, typique des Banquiers centraux et de leur pouvoir discrétionnaire honni : « la fondation Ethereum a poussé le Hard Fork à renflouer les développeurs* de Slockit et d'Ethereum, bien qu'il n'y ait pas de consensus du tout » (WhalePanda 2016).

Au sein de la période de mise en crise, nous conservons un découpage entre une phase d'insémination/gestation et une phase de déclenchement. Si, comme précédemment, elles correspondent à deux étapes distinctes dans leur temporalité et les actions entreprises, les frontières sont plus poreuses. La découverte du bogue sous la forme d'une attaque principale est certes « le » moment du déclenchement de la crise, et c'est elle qui va donner le « tempo » de la remise en ordre à venir. Mais elle a été précédée d'une série d'alertes publiques concernant la sécurité de « The DAO » qui ont amorcé des réflexions sur la remise en ordre. Nous démarrons la périodisation au lancement du protocole Ethereum, le 30 juillet 2015, pour souligner que le contexte de cette crise est celui des premiers temps du protocole Ethereum. Au sein de son écosystème naissant, l'entreprise qui lance « The DAO » et ses membres sont des acteurs centraux et reconnus. L'extension du périmètre de la crise, comme de son intensité, procède de l'engouement suscité au sein de la jeune communauté pour le lancement de « The DAO ». Celui-ci s'est en effet traduit par une levée de fonds record, pour l'un des premiers projets d'ampleur. En ce qui concerne la période de remise en ordre, *a contrario*, nous sortons du découpage entre phase d'évaluation et phase de résolution. Un tel découpage est pertinent pour une crise à gouvernance de « huis clos », mais il ne l'est plus pour restituer la crise présente et l'incertitude entourant sa gouvernance. Le déclenchement de la crise par la découverte d'une attaque en cours ouvre dans l'urgence, pour la communauté « The DAO » et celle d'Ethereum, une période de remise en ordre cacophonique. L'« effet laboratoire » particulièrement présent dans la crise Bitcoin CVE 2018 s'estompe : acteurs et instruments mis en action ne sont pas « *tout puissants* » d'où un « *gouvernement des crises [...] fait de bricolages* », [subissant] *des échecs [...] des imprévus tout au long du déploiement des politiques qu'il expérimente* » (Aquiton, Cabane et Cornilleau 2019, p. 16).

Du fait d'un attaquant actif *et* réactif, mise en crise et remise en ordre vont survenir *on chain**, de façon publique et obliger à réagir en temps réel, produisant incertitude (stratégique, organisationnelle et juridique) et complexité. On est loin du « confort » offert par le secret et la confidentialité d'une gouvernance de « huis clos », déterminant *une* remise en ordre unitaire, cohérente et coordonnée par une poignée d'acteurs de confiance. Ici, l'incertitude et les contraintes (particulièrement temporelles) prédominent et des questions de gouvernance se posent explicitement : des fenêtres d'action sont définies dans les codes de « The DAO » (renseignées en bas de la chronologie et par des aires de couleurs). Elles forcent à des actions rapides et précipitées dans un contexte d'absence de réponse claire aux questions du « qui » est en charge de la remise en ordre et de « comment » et « pourquoi » le faire. Cette crise fait place à *des* remises en ordre, hétérogènes en termes d'acteurs (d'où le grand nombre de groupes d'acteurs y participant, cf. marge de gauche), d'objectifs et de moyens. La cacophonie débouchera finalement sur une résolution sous forme d'une action collective et concertée.

Pour comprendre qu'un bogue touchant au domaine protocolaire conduise à réaliser un *Hard Fork** contentieux de la couche protocolaire, il faut saisir le contexte du développement infrastructurel d'Ethereum qui était encore en phase « de preuve de concept ».

Phase d'insémination : démesure d'un fonds d'investissement distribué sur Ethereum

Comme pour la crise Bitcoin CVE 2018, l'origine de la crise réside dans la présence d'une faille dans des codes informatiques. À la différence du cas précédent, cette crise « de vulnérabilité » ne relève pas du domaine protocolaire, mais du domaine applicatif (cf. section I.2.1 précédente) : les codes d'Ethereum sont hors de cause, la faille étant logée dans ceux d'un *Smart Contract** établissant l'une des premières Organisations Autonomes Distribuées (ou DAO) « *de l'histoire de l'humanité* », sous la forme d'un fonds d'investissement en capital-risque décentralisé « *régi par la philosophie "code is law", par opposition aux mécanismes de contrôle centralisés* » (Bitmex Research 2017b). Cet organisme doit permettre « *aux investisseurs du monde entier de mettre en*

commun leurs fonds, puis de voter sur la manière de les déployer » (David Z. Morris 2023). L'idée et le développement du projet « The DAO » a émergé avant même le lancement d'Ethereum : la création du répertoire Github hébergeant le développement des codes logiciels et le premier *commit* datent de juin 2015⁴⁴¹, soit un mois avant le lancement du « *mainnet* » (la version « *frontier* », cf. Chap. I section I.3.2). Ce projet s'inscrit dans la stratégie de financement d'une start-up : « *Slock It* ». L'entreprise allemande est fondée en septembre 2015⁴⁴² par trois associés, les frères Christoph et Simon Jentzsch et Stephane Tual, qui recrutent deux collaborateurs, Griff Green et Lefteris Karapetsas. L'équipe de développement est ainsi constituée de cinq membres, dont trois participent déjà de l'écosystème d'Ethereum : Tual est à l'époque chargé de la communication d'Ethereum pour la Fondation, C. Jentzsch a travaillé pour elle au développement du langage Solidity⁴⁴³ (avec Christian Reitwiessner et Gavin Wood) et du client C++, au sein de l'équipe de V. Buterin à laquelle participe Karaptesas (Slockit GmbH et Jentzsch 2015, cf. Tableau 9 suivant).

Tableau 9 : L'équipe Slock It

Nom Prénom	Statut(s) et rôle(s) chez « Slock It »	Statut(s) et rôle(s) dans l'écosystème
Jentzsch Christoph	Co-fondateur et directeur de la technologie (« <i>Chief Technology Officer</i> »)	Équipe C++, responsable des tests (« <i>Lead Tester</i> »), « ETH Dev Berlin » & Ethereum
Jentzsch Simon	Co-fondateur et directeur général (« <i>Chief Executive Officer</i> »)	/
Tual Stephan	Co-fondateur et directeur des opérations (« <i>Chief Operating Officer</i> »)	Directeur de la communication (« <i>Chief Communication Officer</i> »), Ethereum
Karapetsas Lefteris	Responsable ingénieur technique (« <i>Lead Technical Engineer</i> »)	Équipe C++, « ETH Dev Berlin » ; « Robin Hood Group » et « White Hat Group » au cours des événements
Green Griff	Organisateur de la communauté (« <i>Community Organizer</i> »)	« Robin Hood Group » et « White Hat Group » au cours des événements

Source : Rolland Maël

« Slock it » ambitionne de « *décentraliser l'économie de partage* » en contestant le monopole des plateformes « *Airbnb* » ou « *Uber* » et leurs « *frais extraordinaires* » : pour ce faire, « *pas besoin de faire fonctionner des serveurs ou de gérer des transactions** [,] de transférer de l'argent ou de gérer la remise des clés. Tout cela sera géré par la blockchain Ethereum » et des *smart contracts** permettant aux usagers de contracter via une plateforme décentralisée et des serrures et

⁴⁴¹

Voir

https://github.com/blockchain*llc/DAO/commits/develop?after=e50d3bc008cf0bbe4285de9dda54d3a541cb0b4+944&branch=develop [consultation au 14/02/2021].

⁴⁴² Voir <https://www.crunchbase.com/organization/slock-it> [consultation au 14/02/2021].

⁴⁴³ C. Jentzsch, actif de 2014 à courant 2016, est le quatrième contributeur au répertoire Github de « *Solidity* », voir <https://github.com/ethereum/solidity/graphs/contributors> [consultation au 19/05/2022].

verrous qui y seront connectés⁴⁴⁴ (slock.it 2016). Le projet est ambitieux. En plus de développer « *la plateforme en déployant le contrat intelligent* sur la blockchain Ethereum et en vendant le matériel qui l'utilise* », il vise aussi à fournir différents services : un explorateur *ad hoc*, l'intégration de méthodes de paiement traditionnelles, des solutions personnalisées, etc. (*Ibid.*). L'entreprise doit être financée et, au commencement, le projet n'est pas encore « *The DAO* », mais une simple ICO qui ne s'« *appelait [même] pas ICO à l'époque [...] On ne savait pas encore... les mots on ne les avait pas encore* » [et] « *la conscience que ça crée une nouvelle forme d'entité s'est construite au fur et à mesure [...] au début c'était, on fait un crowdfunding... [...] puis [:] ah oui, mais si on faisait un token et puis on peut voter et puis machin et puis [...] on se pose de nouvelles questions.* » [A. Roussel, Entretien n°11]. C'est au fil des questions rencontrées par l'équipe « *Slock It* » pour se financer que se construit l'idée d'établir un fonds de capital-risque indépendant et autonome, sans conseil d'experts ou de managers, dédié au financement des entreprises de l'écosystème naissant d'Ethereum.

C. Jentszsch, qui fait partie des premiers à avoir travaillé pour la Fondation Ethereum, sait que « *l'organisation à but non lucratif qui supervise le développement de la blockchain [Ethereum], manqu[e] de fonds* », d'où le fait que « *beaucoup de ses contributeurs sont rapidement partis pour poursuivre des projets connexes* » (David Z. Morris 2023). Le fait qu'une partie des membres de l'équipe soit déjà intégrée au développement d'Ethereum et aux ambitions du projet concourt à leur présence à la « *DEVCON 1* » (conférence annuelle des développeurs*, organisée par l'*Ethereum Fondation*, nous y reviendrons dans une section suivante). En novembre 2014 à Berlin, la DEVCON 0 avait donné lieu à la présentation de recherches entourant la conception du design d'Ethereum. Très suivie de la communauté naissante, la DEVCON 1 de novembre 2015 à Londres est la première édition depuis le lancement d'Ethereum et l'évènement fait la part belle aux recherches appliquées et aux projets ambitionnant d'utiliser Ethereum (environ 400 personnes y participent, Gerring 2016). Le projet de serrure connectée est accueilli avec intérêt. Plus encore, l'annonce d'un financement innovant⁴⁴⁵, ne s'arrêtant pas aux canaux de la finance traditionnelle. En effet, les organisateurs revendentiquent disposer « *maintenant de la blockchain Ethereum et [pensent pouvoir] faire beaucoup mieux* »⁴⁴⁶ : en plus de droits de vote, des avantages pécuniaires seront à « *retirer si vous participez* », « *vous pourrez voter sur les décisions importantes et, surtout, vous contrôlerez les fonds ! [Le] but est d'être une DAO rentable. Il s'agit d'une DAO à but lucratif.* » (Slockit GmbH et Jentszsch 2015) Puisque ce qu'ils « *faisaient était suffisamment intéressant pour intéresser une communauté [choix fut fait de] donner une dimension complètement différente* » au financement de Slock It via la constitution de l'entité « *The DAO* » : leur entreprise ne serait financée qu'en tant que] service provider de cette entité, c'était ça leur but [...]. Ils disaient : « *on développe un truc, on le donne à la communauté et en échange on devient service provider de ce truc-là.* » [A. Roussel, Entretien n°11]. « *Slock It* » développe cette entité comme un véhicule de financement, espérant

⁴⁴⁴ La serrure, dénommée « *Slock* », sera « *connectée au contrat intelligent* Slock de la blockchain* Ethereum et contrôlée [et] le propriétaire [pourra] fixer un montant de dépôt et un prix pour la location [...] et l'utilisateur paiera ce dépôt par le biais d'une transaction [pour obtenir] la permission d'ouvrir et de fermer ce verrou intelligent [avec] son téléphone.* » (slock.it 2016)

⁴⁴⁵ Chaque panel et présentation est diffusé en ligne et en temps réel, puis archivé. Pour la présentation de « *Slock It* », voir <https://archive.devcon.org/archive/watch/1/slockit/?playlist=Devcon%201&tab=YouTube> [consultation au 22/05/2022].

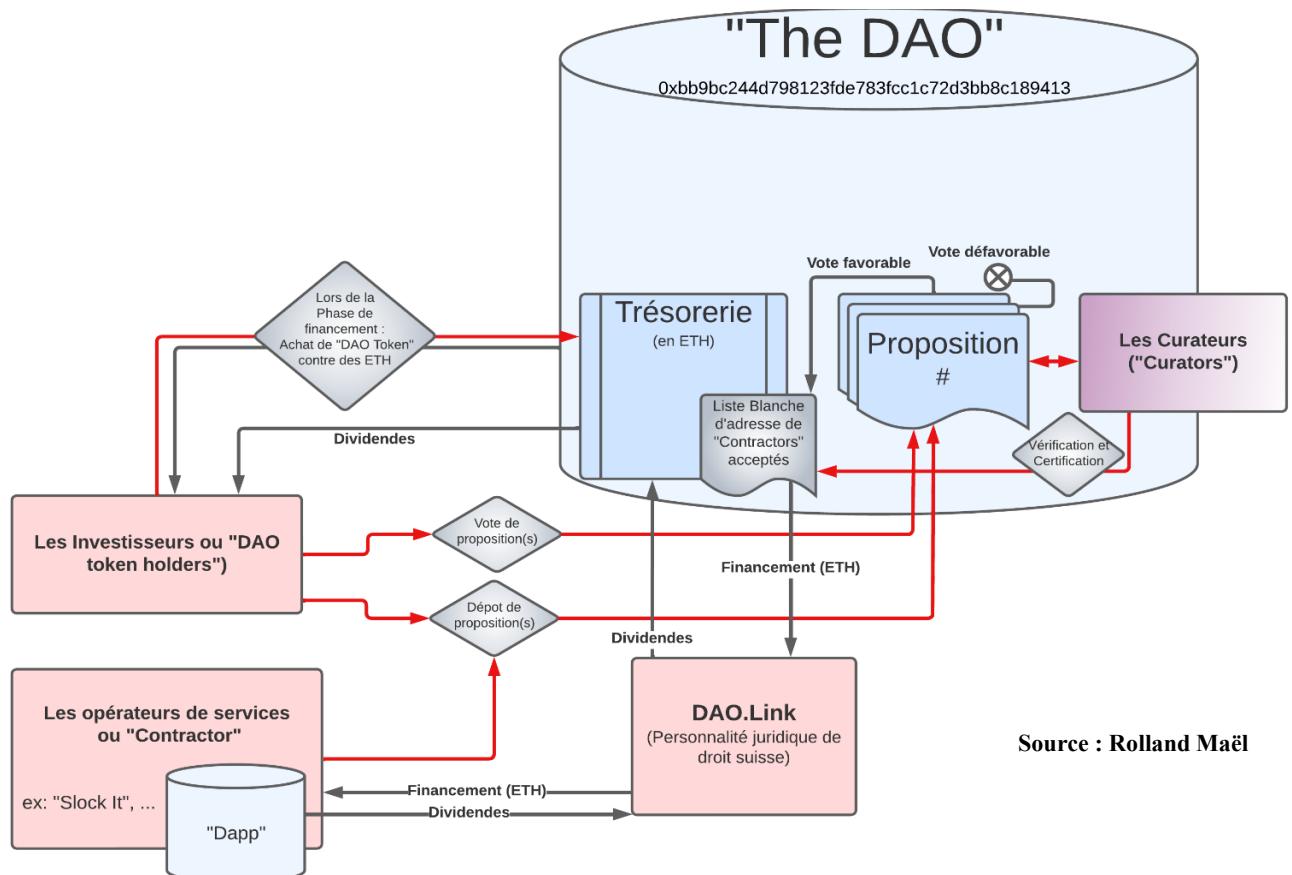
⁴⁴⁶ Jentszsch témoigne de l'intérêt des investisseurs pour « *The DAO* »: « *Nous discutons avec des investisseurs et certains d'entre eux veulent nous donner de l'argent. Comment pouvons-nous gagner de l'argent ? [...] Nous n'avons pas besoin de le faire à l'ancienne. [...] Bien sûr, il faut que ce soit une DAO ! [...] Quelles sont les tâches de la DAO ? Tout d'abord, elle finance le développement. Nous ferons une prévente, une collecte de fonds, un crowdfunding. C'est là que nous avons besoin de votre aide* » (Slockit GmbH et Jentszsch 2015). Notre entretien avec A. Roussel [Entretien n°11] confirme cet engouement.

être « *au début [ce] fournisseur de services, mais en fait [la DAO et ses membres seront] libres de choisir le fournisseur de services qu'ils veulent* » (*Ibid.*). « Slock It » ne sera à terme qu'un de ses prestataires ou « *contractor* », acteurs humains que la DAO doit engager afin d'« *exécuter des actions dans le monde réel* », car la DAO en tant que « *logiciel pur* » (Teruzzi 2016a), « *ne peut pas construire un produit, écrire un code ou développer du matériel.* » (Jentzsch 2016b)

À partir de l'introduction publique de la *Devcon*, les projets de « Slock It » et de DAO d'investissement ne cesseront de croître, comme l'intérêt qu'il suscite au sein de la communauté Ethereum. « Slock It » continue d'assurer la promotion du projet *via* la publication d'informations sur son blog : en mars, S. Tual (2016a) publie un billet se voulant être « *une introduction de haut niveau au cadre standard DAO et à son White Paper** ». La communauté se structure d'abord *via* le forum « *Slack* », créé par « *Slock It* » et conçu comme le canal de discussion principal. En février, on compte une multiplicité de canaux linguistiques différents (communauté polonaise en tête), fin mars le « *canal général de The DAO comport[e] près de trois mille membres* » (Shin 2022, p. 125) et culminera à près de 5 000 (Jentzsch 2016c). En mars 2016, le *White Paper** est rendu public, suscitant un engouement renouvelé (Falkon 2017) : revenant d'abord sur le concept de DAO, il décrit et propose la version standardisée d'une « *première implémentation* » d'« *un code de contrat intelligent* standard [permettant de] former une organisation autonome décentralisée (DAO) sur la blockchain Ethereum.* » (Jentzsch 2016b) Ce code est un « *modèle même de simplicité, avec à peine 900 lignes de code source* » (DuPont 2018, p. 2). Il annonce « *automatiser la gouvernance et la prise de décision au sein d'une organisation [...] en utilisant des contrats intelligents écrits en Solidity* » (Jentzsch 2016b). Le *Smart Contrac*t TheDAO v.1* constitue un ensemble de règles et de dispositifs organisationnels formalisant le fonds et son administration, établissant un ensemble de statuts, rôles et actions légitimes en son sein (cf. Figure 13).

« The DAO » représente un fonds de trésorerie abondé lors d'une phase préliminaire dite « *de création* » durant laquelle seront émis les tokens « The DAO » contre des Ether. Tout détenteur d'ETH pourra devenir investisseur dans « The DAO » et dans les projets, qui demanderait à être « *Contractor* » via un processus de proposition cadré. La gestion du fonds relève directement de ses investisseurs, membres formels en tant que porteurs du jeton « The DAO » (ticker – DAO), qui sont les seuls à décider quel projet sera financé avec leurs fonds et selon quelles modalités, car ils bénéficient des droits suivants : proposer des projets à financer, voter pour ou contre des projets demandant des financements et recevoir des dividendes des projets financés, qui versent des revenus au fonds « The DAO » en contrepartie de leur financement, ensuite réparti aux porteurs en proportion de leur possession dudit Token (*Ibid.* ; Chohan 2017 ; DuPont 2018). Quatre statuts différents existent : les porteurs de jeton DAO (« DAO Token Holders ») ; les prestataires (ou

Figure 13 : Statuts, rôles et fonctionnements clefs de « The Dao »



Source : Rolland Maël

L'intérêt communautaire large pour la structure proposée se traduit par la publication d'informations excédant l'équipe de développement : S. Polrot, pour la communauté Ethereum France présentera, par exemple, les *promesses* du projet (Polrot 2016b). Le choix innovant de « Slock It » de n'être qu'un prestataire parmi d'autres du fonds « The DAO » s'inscrit dans l'éthos de décentralisation, et offre aussi une protection juridique à l'équipe. Il impose de structurer la communauté au-delà de la start-up. Des membres actifs du *Slack* existant, « *Felix Albert et Auryn Macmillan [...] rejoint par une équipe Core de six autres membres* »⁴⁴⁷ (DuPont 2018, p. 2) créent un forum indépendant, « *DaoHUB.org* » (Auryn 2016). « Slock It », via Tual, est « très satisfait » : « *les forums de Daohub.org sont un excellent* » outil, servant à fournir des informations et conseils

⁴⁴⁷ Les membres sont : Felix Albert, Auryn Macmillan, Boyan Balinov, Arno Gaboury, Michal Brazewicz, Taylor Van Orden-Monahan, Des Donnelly, Daniel McClure (Auryn 2016 ; Bitmex Research 2017b).

aux nouveaux usagers, ainsi qu'à proposer et débattre des propositions (lucratives ou non) à soumettre à « The DAO » (Tual 2016b). Début avril sont dévoilés les résultats de l'audit des codes de la V1.0 de « The DAO », réalisé par l'entreprise « déjàvu » (celle qui avait audité les codes du protocole Ethereum pour la Fondation Ethereum) (Tual 2016a) : pas de problème notable. Mais la sécurité ne tient pas qu'au code. Puisque l'entité « The DAO » est indépendante vis-à-vis de « Slock It », « le fournisseur de services par défaut de la DAO devrait être remplacé par un ensemble de curateurs indépendants » (Jentzsch 2016c), garantissant une sécurité minimum, en assurant la sélection des équipes et projets demandant des financements au fonds (Teruzzi 2016a). Ce statut de « Curators » s'incarne dans une liste d'adresses à fonction particulière, liée à des acteurs humains reconnus et de confiance devant vérifier l'authenticité de l'identité des personnes (physiques ou morales) qui souhaitent réaliser des transactions* avec l'entité « The DAO » : c'était « une sorte de contrôle KYC », un « contrôle humain, pour s'assurer que les adresses mises sur liste blanche, qui pourraient recevoir beaucoup d'argent, [appartiennent bien aux] personnes [déclarées] », et le rôle attendu des personnalités choisies est « de... whitelister des adresses, si la DAO veut financer un projet quelconque, c'est nous qui devrions dire, cette adresse appartient à ce projet et maintenant les électeurs de la DAO peuvent voter. Nous ne votons pas, nous ne décidons pas, nous ne faisons rien d'autre que de mettre ou non des adresses sur liste blanche » [Fabian Vogelsteller, Entretien n°12]. Leur rôle est conçu comme « trivial et purement technique », pouvant « être remplacé à tout moment » au bon vouloir des possesseurs de DAO token (Wood 2016). Le 25 avril est annoncée la liste des « experts bien connus de la communauté Ethereum [...] portés volontaires pour faire ce travail » (Jentzsch 2016c) : « en partenariat avec Daohub.org, [« Slock It » obtient] un ensemble de signataires du curateur de la DAO qui ressemble au Who's Who de la cryptographie* [avec] 11 membres [...] tous des membres actuels ou anciens du projet Ethereum » (Tual 2016d), dont le fondateur d'Ethereum lui-même⁴⁴⁸, « ce qui a donné au projet une traction supplémentaire » (Jentzsch 2016c). Les codes sources de « The DAO » sont ouverts au public le 29 avril. Publié sous licence libre, ces codes, bien que majoritairement écrits par C. Jentzsch et L. Karapetsas, ont vu près de 18 contributeurs participer à leur rédaction sur le répertoire Github⁴⁴⁹. Pour définitivement asseoir le caractère décentralisé de l'entité « The DAO » et son autonomie vis-à-vis de « Slock It », le déploiement des codes, par réalisation de transactions* dédiées, est laissé à l'initiative d'anonymes de la communauté. Le 30 avril, 8 instances des codes ont été déployées selon les consignes préalablement données sur le forum DAOhub et celle choisie par « DAOhub.org » pour devenir

⁴⁴⁸ Les 11 « Curators » sont : V. Buterin, Inventeur et fondateur d'Ethereum, Ethereum Foundation ; G. Wood, Fondateur d'Ethereum et d'Ethcore ; C. Reitwießner, Chef d'équipe Solidity & C++, Ethereum Foundation. ; A. Van de Sande, Designer en chef, Mist, Ethereum Foundation ; V. Tron, Développeur principal client Go, Ethereum Foundation ; A. Buchanan, Responsable de la recherche et du développement, Ethcore et EthDev, Berlin ; T. Gerring, Directeur de la technologie, Ethereum Foundation ; M. Becze, Développeur client JS et la R&D sur l'EVM, Ethereum Foundation ; G. Simonsson, Développeur principal, Ethereum Foundation ; V. Zamfir Recherche PoS (Casper), Ethereum Foundation ; F. Vogelsteller, développeur principal Mist et l'API web3.js, Ethereum Foundation (Tual 2016d).

⁴⁴⁹ Par ordre décroissant en quantité de commits : C. Jentzsch, Letteris Karapetsas, Yoichi Hirai (aka pirapira) ; Griff Green ; Hayden Colm (aka « CryptoColm ») ; Simon Jentzsch ; Zhangyaning (aka « u2 »), J. Baylina, Pawel Bylica (aka « chfast »), Stephan Tual, Paul Schmitzer (aka « LiteBit ») ; Jeffrey Anthony ; Christian Reitwiessner aka « Chriseth »), Pierre-Elouan Réthoré (aka « rethore »), Anthony Akentiev , Isidoro Ghezzi (aka « isghe »), Eric Fish (aka « mrefish ») et Gustav Simonsson. Voir <https://github.com/blockchainsllc/DAO/graphs/contributors> [consultation au 14/02/2021].

canonique est tirée « à pile ou face » entre deux adresses sélectionnées pour leurs conditions de pseudonymat renforcées⁴⁵⁰ (Tual 2016a).

Ce même jour, « *The DAO* [entre] en ligne et [...] dans sa phase de création à l'adresse 0xbb9bc244d798123fde783fcc1c72d3bb8c189413 » (*Ibid.*), qui est programmatiquement ouverte pour 28 jours : la « crowdsales » est lancée jusqu'au 28 mai, il devient possible de créer des DAO tokens en envoyant des ETH à « *The DAO* »⁴⁵¹. Les premiers *DAO Token Holders* agissent moins par confiance que par foi, envoyant, sans diligence raisonnable (contenue dans l'injonction DYOR) aucune, « plus de 1 537 000 ethers [...] au contrat intelligent* de la *DAO*, [alors même que personne ne sait] si le code source du contrat est correct » : heureusement, l'instance choisie est conforme aux codes publiés, en particulier les adresses de curateurs qui y sont stipulées coïncident avec celles publiquement annoncées (DAOhub 2016). Là où les membres « *Slock It* » avaient conçu « *The DAO* » « comme un mécanisme de collecte de fonds » pour eux seuls et s'attendaient à lever « quelque chose comme 5 à 10 millions de dollars », « les choses ont rapidement dérapé alors que le buzz autour de *The DAO* s'accélérerait [:] l'objectif est rapidement et « largement dépassé, [et c'est après] avoir récolté 20 ou 30 millions de dollars [, qu'] on est passé du financement de *Slock.it* au financement de toutes les applications sur Ethereum » (Jentzsch cité par David Z. Morris 2023). Si J.R. Willet avait inventé l'ICO pour financer Omni/MasterCoin (cf. Chap I), « *The DAO* », en « établissant le record de la plus grande campagne de crowdfunding de l'histoire à l'époque » (Insider 2021, voir Annexe n°I.4), fait gagner ces lettres de noblesse à ce type de financement. Son attaque va permettre d'identifier de bonnes et mauvaises pratiques. Nombreuses sont les personnes que le projet va intéresser et même exciter⁴⁵². En témoigne A. Roussel, qui va avec son associé Gian Botshler : « [s'] intéress[er] à *Slock It*. C'était un projet qui était en vue, il était intéressant [...] on a fait partie de cette communauté de gens qui était absolument hallucinés par ce qui était en train de se passer [...] On a voulu participer » [A. Roussel, Entretien n° 11]. Cette volonté d'investissement va se muer en un partenariat entre la plateforme d'échange Suisse Bity et « *Slock It* » (Roussel 2016c), permettant d'ouvrir une passerelle* simplifiée pour les novices, leur

⁴⁵⁰ Déployer une instance de *Smart Contract** via une transaction nécessite des UCN ETH pour les frais de transaction afférents à l'opération. Les conditions d'approvisionnement en ETH du compte sont déterminantes dans la préservation de l'anonymat de la/des personne(s) impliquée(s) ; elles pourraient être attachées à des données *off chain** (adresse IP, adresse mail, ID, etc.). Un tutoriel de la procédure de déploiement de « *The DAO* », couvrant cette anonymisation, est publié sur le forum DAOHub (voir <https://forum.daohub.org/t/the-dao-official-bytecode-deployment-and-pushing-the-big-red-button-thread/519> [consultation au 14/02/2021] et sur le Slack (le 29 avril) : « Hey tout le monde. Si vous voulez déployer le *DAO*, regardez ce fil de discussion. Nous allons en choisir un au hasard dans ce fil pour être la *DAO* officielle très bientôt. Procurez-vous des pièces intraçables / sans historique (ShapeShift, btc mixer, etc.) et déployez. » (T. Monahan cité par Shin, 2022, p. 131).

⁴⁵¹ La levée de fonds se déroule en trois phases : les 15 premiers jours, le ratio était de 1 ETH/ 100 DAO Tokens, ensuite le nombre de tokens reçus diminue progressivement chaque jour avant la dernière phase des 4 derniers jours, où 100 Dao Tokens valaient 1,5 ether. L'excédent des investisseurs contribuant à plus de 1 ETH pour 100 DAO Tokens est alloué à un compte spécial appelé extraBalance (Jentzsch 2016b).

⁴⁵² Tous les acteurs rencontrés soulignent cette excitation. *Idem* du côté des académiques : pour nous, c'était la première participation à une ICO sur Ethereum ; même excitation de notre collègue A. Slim, nous racontant s'être procuré des DAO Tokens via Kraken. Dupont (2018) aussi y participera et va même proposer la création d'une « organisation caritative environnementale [...] "The DAO of Whales" [visant à prendre soin] de baleines oranges dans le nord-ouest du Pacifique » (DuPont 2018, p. 5).

permettant d'accéder à l'ICO, *on chain** mais en fiat monnaie⁴⁵³. Un autre partenariat crucial s'est noué entre eux à quelques jours de l'ICO, prenant la forme d'une entreprise, « DAO.Link », « SARL » créée comme « *un Join Venture 50/50* », elle permet de résoudre le dernier « *blocage [que l'équipe] avait* »⁴⁵⁴ [A. Roussel, Entretien n° 11] : « *Slock It* » et tout « *Contractor* » passeront via cette entité *Ad Hoc* de droit suisse pour contracter légalement avec « *The DAO* », car « *les factures et les bons de commande des entreprises ont besoin d'une adresse physique et - soyons réalistes - "The DAO, Ethereum blockchain smart contract address 0x93139adb39alf...dd031" ne fera pas l'affaire de votre bureau local des impôts* » (Tual 2016e). À l'accès facilité pour les investisseurs à l'ICO s'ajoute celui à des marchés secondaires. Dès le 27 mai, la bourse Kraken annonce ouvrir des marchés secondaires pour le DAO token dès qu'il deviendra transférable, le 28, devenant « *l'une des premières grandes bourses internationales à échanger des tokens DAO* [et ce, relativement à] *cinq monnaies fiduciaires différentes* » (Kraken et Southurst 2016). D'autres bourses suivent, comme « *Gatecoin, Bity, ShapeShift et Bittrex* » (De Tychy 2016). Dans le même temps, le traitement médiatique est large, la curiosité pour cette « *entreprise automatisée [levant] l'équivalent de 120 millions de dollars en monnaie numérique* » (Waters 2016) excède les cénacles *coiners** et leurs publications spécialisées : à cet article de Waters du *Financial Time* le 06 mai s'ajoute celui de Popper (2016) pour le *New York Times* du 22 mai. Tout concourt à une participation massive qui n'a pas été anticipée : au montant minimum programmé pour que la levée de fonds soit valide (Jentzsch 2016b) ne répond aucune limite maximale (Buterin 2016e), d'où une ICO de tous les records : près de 11 994 260 ETH, équivalents à près de 16% de la masse monétaire en circulation, ont été mis en commun pour une valeur de près de 150 millions de dollars à l'époque par environ 6 700 adresses uniques (Castillo 2016 ; Waters 2016 ; Quentson 2016). Ce succès bénéficie aussi à Ethereum et à son UCN* l'Ether, dont le cours passe « *d'environ 7,50 dollars lors du lancement de la DAO [à près] de 12 dollars à la clôture de la DAO le 28 mai, soit un bond de 60%* » (Shin 2022, p. 134). À mesure que « *The DAO* » suscite « *beaucoup d'enthousiasme dans l'écosystème crypto* » (Bitmex Research 2017b), les inquiétudes grandissent ; en témoigne, le 13 mai, la défection de G. Wood au poste de « *Curator* », qui justifie son choix par des craintes de réputation liées à « *l'utilisation du terme "curateur"* », pour lui « *trompeuse, suggérant une certaine autorité pour un jugement indépendant* », donc des responsabilités, là où « *les deux propriétés essentielles d'une DAO sont qu'elle est décentralisée et qu'elle est autonome* » (Wood 2016)...

Le déclenchement : des alertes variées précédant l'attaque de « *The DAO* »

En cette fin du mois de mai 2016, les derniers jours de l'ICO, pour autant qu'ils ne sont pas « le » moment du déclenchement de la crise à venir, s'y lient inextricablement. Certains

⁴⁵³ Cet arrangement permet « *de payer en euro, en dollars ou en francs suisse [...] On faisait vraiment les choses bien, [...] tout on chain*, la personne nous déclarait une adresse ether [...]. Tu envoyais tes euros. À ce moment-là, on te quotes un prix en Ether et [...] on fait deux transactions [...] une transaction du montant d'Ether, de 100 balles [...] on envoie 99 euros équivalent Ether vers la DAO mais avec transfert, en ajoutant cette fonction particulière [...] create by proxy donc on attribuait les tokens au wallet de la personne. Et [...] on envoyait l'équivalent de 1 euro d'Ether à la personne [...] qu'il ait un petit peu d'Ether pour faire bouger son token, parce que du coup... Il y a eu beaucoup de gens c'était la première [, ils] voulaient participer à la DAO sans avoir d'Ether, ils ne savaient pas. [...] Je crois qu'il n'y avait que deux boîtes qui ont fait cela.* » [A. Roussel, Entretien n°11].

⁴⁵⁴ Ils « *voulaient tout bien organiser hein, ils ont vraiment fait ça de manière professionnelle, c'est des ingénieurs et tout, ils ont tout bien fait. Et à moment donné, quelqu'un leur a dit [...] Mais la DAO, est-ce qu'elle a un numéro de TVA ? Puis ils ont dit ben non ! Et là on leur a répondu, bien alors vous ne pouvez pas faire du business avec vous, puisque vous, en tant que société allemande, vous devez avoir comme contrepartie une société qui a un numéro de TVA. Et ça les a complètement bloqués. [...] Il y avait tout le code [...] en préparation, ils corrigeaient les derniers bugs, enfin bon, il y a eu des bugs mais, heu.. ils faisaient les derniers ajouts, la communauté était prête, tout le monde était prêt. Le business model était prêt, l'ICO était prête, [pour ne pas pouvoir] finalement faire ce qu'on veut, parce que il y a pas de numéro de TVA* » [A. Roussel, Entretien n°11].

« aficionados [...] craignent que le code de l'organisation n'ait été élaboré relativement hâtivement [,] les jeunes machines complexes ont tendance à avoir des failles et des vulnérabilités que l'on ne peut pas anticiper » (J. Lubin, cité par Popper 2016b). Les premières alertent n'attendent pas la fin de l'ICO pour éclater publiquement. Pour « Slock It », « The DAO » et les membres de leur communauté, la crise commence...

Le succès de la levée de fonds conduit le contrat de « The DAO » à devenir involontairement un « *pot de miel*⁴⁵⁵ » : autant d'argent au même endroit attire l'attention, et pas seulement de personnes bien intentionnées. Des personnes bien intentionnées d'abord. De l'aveu de Zamfir [Entretien n° 9], chercheur pour la Fondation Ethereum et membre des « *Curators* » de « The DAO », la diligence raisonnable fut trop tardive, pour lui comme pour d'autres, et « *malheureusement [...] on a regardé une fois seulement après qu'il y ait eu beaucoup d'argent* » : « *j'ai commencé à m'inquiéter parce que je ne savais pas comment fonctionnait la DAO, qui était vraiment impliqué, ce qui se passait, rien du tout.* » [V. Zamfir, Entretien n° 9]. Zamfir fait partie du groupe de chercheurs en sciences informatiques qui publie le 26 mai un billet de blog relevant des problèmes de design (Sirer, Mark et Zamfir 2016). L'analyse ne regarde pas le code, mais les incitations structurelles en termes de théorie des jeux. Le design et les mécanismes de vote sont problématiques. Ces derniers induisent différents vecteurs d'attaques⁴⁵⁶ pouvant « *conduire à des manipulations financières, voire à des pertes* », et, puisque « *l'étude a identifié des solutions potentielles pour atténuer ces biais et vulnérabilités* », les auteurs proposent un « *moratoire temporaire* » sur toutes les propositions qui seraient soumises à « The DAO », jusqu'à ce qu'une nouvelle version corrigée soit développée, acceptée et implantée (*Ibid.*). Cette alerte ne reste pas confinée et, le même jour, un article du *New York Times* revient sur les vulnérabilités qui viennent d'être publiées (Popper 2016a). Les conditions de cette divulgation posent question. Pour certains, il est « *bizarre* » que « *Gun Sirer et Vlad Zamfir [aient] publié cette vulnérabilité d'abord dans le New York Times, avant de parler à Christoph et aux parties impliquées ? [...] C'est la pire chose à faire parce que cela a immédiatement attiré l'attention de tous les pirates et escrocs du monde sur The DAO parce que c'est le oh wow* » [Entretien SuperAnon]. D'après Zamfir, la divulgation est responsable, « *tous les curateurs et la team* » ont été informés au « *plus vite qu'on pouvait* », avant la publication : différents canaux sont mobilisés (Skype, mais aussi email) pendant « *deux jours [pour] essayer d'obtenir un accord politique, [...] entre Slock It et les curateurs pour avoir un moratorium* » [V. Zamfir, Entretien n° 9]. La « *team Slock It n'a pas vraiment apprécié la sortie du document, [...] ils pensaient que c'était quelque chose qu'[il aurait fallu] faire plus tôt* » [*Ibid.*]. Le timing de cette publication n'est pas idéal, puisqu'elle intervient un jour avant la fin de la *période de création* ouvrant sur celle de proposition et de vote [*Ibid.*, F. Vogelsteller, Entretien n° 12 ; Jordi Baylina, Entretien n° 7]. Impossible d'intervenir maintenant. Le moratoire temporaire est acquis chez les curateurs, et le mieux aurait été de gagner du temps afin de « *réfléchir à une stratégie de mise à niveau* » en taisant cette publicité [Entretien SuperAnon].

Ce papier du « *Moratorium n'a pas parlé de la réentrance, la réentrance est une question très technique [...] cela n'a rien à voir avec... ce social... c'était une chose très différente* » [Jordi

⁴⁵⁵ Un « *pot de miel* », en sécurité informatique, est unurre conçu pour attirer les attaques informatiques. Dans ce cas, les 150 millions de dollars d'ETH du contrat agissent non intentionnellement comme tel, attirant les attaquants potentiels.

⁴⁵⁶ Différentes versions du papier existent (Sirer, Mark et Zamfir 2016 ; Mark, Zamfir et Sirer 2016) et malgré des divergences marginales, les vecteurs d'attaque identifiés sont : « *Le biais affirmatif et la désincitation au vote non* » ; « *L'attaque par harcèlement* » ; « *L'attaque par embuscade* » ; « *Le raid sur les jetons* » ; « *L'attaque par déséquilibre* » ; « *L'attaque par fractionnement de la majorité* » ; « *L'attaque simultanée par ligotage* » ; « *L'hypothèse d'indépendance* » ; « *La dilution des récompenses* » ; « *Le vote sans risque* » ; « *Le piège de la proposition simultanée* ».

Baylina, Entretien n° 7]. Mais début juin, ce sont les codes qui commencent à être éprouvés, indirectement d'abord. Le 5, l'architecte principal du langage de programmation* d'Ethereum, Solidity, annonce y avoir « *découvert un anti-modèle [...] qui pourrait conduire à des attaques sur les contrats intelligents* » (Jentzsch 2016c). Sa découverte, il l'explique par la jeunesse d'Ethereum dont le développement infrastructurel n'est encore qu'en phase de « *Preuve de concept* » : « *lancé en octobre 2014, alors que ni le réseau* Ethereum, ni la machine virtuelle n'avaient fait l'objet de tests en conditions réelles [...], certaines des premières décisions de conception [de Solidity, NDA] étaient initialement considérées comme les meilleures pratiques [, mais] confrontées à la réalité [,] certaines d'entre elles se sont révélées être des anti-modèles* » (Reitwiessner 2016). Soulignant le manque relatif de relais médiatique à l'époque (cf. « *comme la plupart des gens ne suivent probablement pas le flux des commits github sur ce dépôt* »), Reitwiessner vise à « *mettre en évidence certaines des conclusions ici* » : dans l'exemple de code qu'il donne, « *pendant que la fonction d'envoi est toujours en cours, le destinataire peut rappeler withdrawRefund [...] et il recevra donc à nouveau le montant, et ainsi de suite* » (*Ibid.*). Le 9 juin, le chercheur « Peter Vessenes [...] écrit un blog sur la découverte de Christian » (Jentzsch 2016c) où l'immaturité du développement infrastructurel d'Ethereum apparaît cuisamment. Le billet de blog commence en précisant que « *Chriseth, sur github, a attiré l'attention sur une terrible attaque contre les contrats de portefeuille* » et que s'« *il existait une voie de divulgation responsable pour les développeurs* de contrats Ethereum* », l'auteur l'utilisera, mais pour l'heure, « *il ne semble pas y en avoir* » (Vessenes 2016b). L'annonce de Vessenes a de quoi inquiéter. La vulnérabilité de la « *course au vide* » (« *Race-To-Empty* »), ou « *bogue de réantrace* », est une « *véritable menace* », malheureusement « *très répandue* » : « *votre contrat intelligent* est probablement vulnérable au vidding si vous gardez une trace des soldes des utilisateurs et que vous n'avez pas été très, très prudent* » (*Ibid.*). Le problème réside dans « *une fonction par défaut* » présente dans les « *codes de portefeuilles** » et induisant une mauvaise comptabilisation des retraits : plusieurs retraits peuvent être déclenchés sans que la balance de l'usager n'en soit affectée et, quand « *le code est résolu, le solde de l'utilisateur est fixé à 0, quel que soit le nombre de fois que le contrat a été appelé* » (*Ibid.*). À « *ce stade, l'ensemble de la communauté des développeurs* d'Ethereum [est mise] au courant de ce problème* » (Jentzsch 2016c) et les développeurs* de différents projets s'y intéressent. Le 11 juin, l'équipe de développement de « *MakerDAO* » (sur lequel repose l'émission du stablecoin DAI, cf. Chap. II section II.2.3) découvre qu'un de leurs *Smart contracts** y est exposé, permettant « *à n'importe qui de le drainer* » : en guise de remédiation, ils drainent eux-mêmes les fonds à risques pour les sécuriser (i3nikolai 2016) et gratifient P. Vessenes d'une récompense (« *Bug Bountie* ») en plus de remerciement (i3nikolai 2016b). C'est le 12 juin que le diagnostic est finalement posé pour « *The DAO* » : l'utilisateur « *Eththrowa* », membre du forum DAOHUB, a « *trouvé ce même antipattern dans la DAO, dans la section récompense du code* » (Jentzsch 2016c). L'annonce publique du diagnostic est faite par « *Slock It* » le même jour et se veut rassurante : « *Aucun fonds de la DAO n'est menacé suite à la découverte du bug du contrat intelligent* Ethereum "recursive call"* » (Tual 2016f). Pour l'équipe, « *ce qu'il faut en retenir [, c'est qu'] il n'y a pas d'éther dans le compte de récompenses de la DAO, ce problème ne met PAS les fonds de la DAO en danger aujourd'hui [, mais] cela pourrait cependant nécessiter une reconsideration du Proposal Framework 1.0 avant le déploiement d'un DAO Framework 1.1.* » (*Ibid.*). Le diagnostic n'a mis au jour un problème de réentrance que pour « *le mécanisme de récompense [pour lequel] une solution de contournement était disponible[, d'où le désormais] fameux message "no-funds-at-risk"* » (Jentzsch 2016c). Si « *le cadre [de la mise à jour v1.1, NDA] a été rapidement corrigé en quelques heures* », reste que « *la base de code déployée n'a évidemment pas pu être modifiée aussi rapidement* », car c'était « *un processus lourd qui nécessitait un délai de vote de 2 semaines et une majorité des détenteurs de jetons pour voter* » (*Ibid.*).

Jusqu’alors, comme pour la crise Bitcoin CVE 2018, cette faille, bien que « de vulnérabilité », n’est pas activée, et l’équipe et la communauté pensent encore avoir du temps. Mais, c’est sans compter qu’un attaquant lui, ne manque pas, comme eux, d’identifier un « *exploit similaire dans la fonction splitDAO* » (*Ibid.*). Au petit matin du 17 juin, une attaque est lancée impliquant cette fonction, qui est un dispositif innovant conçu par « Slock It » pour protéger les investisseurs du problème de « *dictature de la majorité* » auquel fait face « *chaque DAO [:] la possibilité pour la majorité de voler la minorité en changeant les règles de gouvernance et de propriété [...]. Par exemple, un attaquant possédant 51% des jetons [DAO] pourrait proposer de s’attribuer tous les fonds [et, détenant] la majorité des jetons, il serait toujours en mesure de faire passer ses propositions* » (Jentzsch 2016b, p. 2). Comme le statut de « *Curators* », cette « fonction split » est pensée pour réguler un comportement considéré comme illégitime en assurant à « *la minorité* » la pleine capacité « *de récupérer sa part des fonds* » : « *si un individu ou un groupe de détenteurs de jetons n'est pas d'accord avec une proposition et veut récupérer sa part d'Ether avant que la proposition ne soit exécutée, ils peuvent soumettre et approuver un type particulier de proposition pour former une nouvelle DAO [dite « Child DAO » et ceux] qui ont voté pour cette proposition peuvent alors diviser la DAO en transférant leur part d'Ether vers cette nouvelle DAO* » (*Ibid.*). La DAO enfant ainsi déployée suivant le cadre prédéfini est alors autonome, mais reprend la structure de la DAO mère : l’ensemble des mécanismes sont les mêmes sauf qu’il faut définir de nouveaux « *Curators* ». Réaliser une proposition de split était la première étape de l’attaque. Elle fut réalisée le 08 juin via « *la proposition DAO #59, avec le titre "Lonely, so Lonely"* », comme révélée par la première analyse de l’attaque de Daian⁴⁵⁷ publiée le 18 juin (2016). L’attaque suit ce déroulement : « *1. Proposer un split et attendre que la période de vote expire [...] 2. Exécuter la scission. [...] 3. Laisser la DAO envoyer à votre nouvelle DAO sa part de tokens [...] 4. S'assurer que la DAO essaie de vous envoyer une récompense avant qu'elle mette à jour votre solde mais après avoir fait (3). [...] 5. Pendant que le DAO fait (4), exécuter à nouveau splitDAO avec les mêmes paramètres qu'en (2) [...] 6. La DAO va maintenant vous envoyer plus de child tokens, et aller retirer votre récompense avant de mettre à jour votre solde. [...] 7. Retour à (5) ! 8. Laissez la DAO mettre à jour votre solde. Parce que (7) retourne à (5), il ne le fera jamais :-)* » (*Ibid.*).

Le 17 juin, à « *T 7 ou 8 heures, heure de Berlin, Griff s'est réveillé et a vérifié son téléphone [:] un membre de la communauté Slack nommé Mo [lui apprenait] que quelque chose d'étrange se passait avec la DAO [,] les fonds étaient en train d'être drainés. Griff a vérifié : un flux de transactions* de 258 ETH (5 600 \$) quittait la DAO.[...] Il a appelé les autres membres de Slock.it. Mo a réussi à joindre le frère de Christoph, Simon, et Griff l'a imploré de prévenir Christoph au plus vite* » (Shin 2022, p. 141). Simon Jentzsch préviendra son frère Christoph qui, sans arriver à « *comprendre immédiatement ce qui se passait* » avec ce split de la DAO principale, était certain « *que quelque chose n'allait pas du tout* » (*Ibid.*). À 9h10, heure de Paris, l’utilisateur « ledgerwatch » annonce la même découverte sur le forum Reddit : « *Je pense que TheDAO est en train de se vider en ce moment [...] je ne peux pas enquêter, mais il semble qu'il s'agisse d'une sorte d'exploit d'appel récursif* »⁴⁵⁸. La crise vient de se muer en crise « de vulnérabilité » et la remise en

⁴⁵⁷ Voir la transaction ici : <https://etherscan.io/tx/0x5798fbc45e3b63832abc4984b0f3574a13545f415dd672cd8540cd71f735db56> [consultation au 12/05/2024]. L’investigation de Shin (2022, p. 148-151) démontre que cette proposition de split émanait d’un investisseur chinois honnête et, le « *mercredi 15 juin, à 6h26 (heure de Berlin), l'attaquant, utilisant deux contrats différents, a voté en faveur de la DAO enfant 59 [...] qui était actuellement vide [et] plus d'une heure plus tard, la période de vote de sept jours sur la Child DAO 59 s'est terminée [et] personne d'autre ne pouvait y entrer. Étant donné que le détenteur chinois de jetons DAO n'avait jamais voté en faveur de sa propre proposition, l'attaquant DAO était la seule personne à pouvoir se séparer de cette DAO.* »

⁴⁵⁸ Voir https://www.reddit.com/r/ethereum/comments/4oi2ta/i_think_thedao_is_getting_drained_right_now/ [consultation au 12/05/2024].

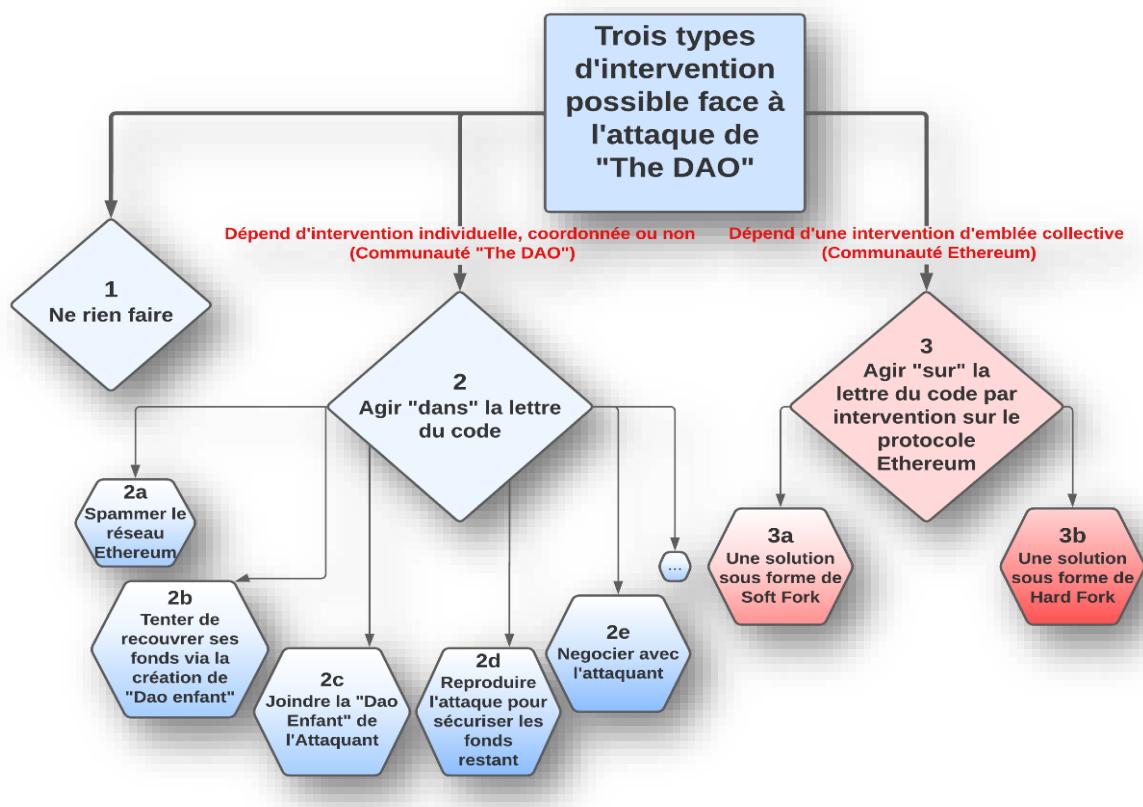
ordre commence, dans la panique. En ce vendredi matin de juin 2016, nombreux sont ceux (comme nous) à se réveiller à la manière de Griff Green et à découvrir en temps réel l'attaque, le krach du cours DAO Token et surtout celui de l'Ether qui s'en suivent⁴⁵⁹. Au-delà d'Ethereum, l'ensemble des communautés *coineuses* est en émoi à la découverte des informations qui commencent à se répandre sur les réseaux* sociaux. Finalement, les délais programmés au sein du *Smart Contract* laissent « *35 jours avant que le pirate ne puisse accéder aux fonds [laissant] le temps [...] à la communauté de réagir... et de se déchirer* » (Polrot 2016c).

⁴⁵⁹ A. Roussel [Entretien n°11] « *organisai[t] une séance avec une dizaine de personnes pour leur montrer ce que c'était la DAO et puis le hack s'est passé en même temps ça c'était genre fantastique. [...] je leur montre, ha regardez [,] c'est quand même bizarre, le nombre d'Ether il descend. [On rigole] Et puis là, un de mes collègues qui commence à regarder les news* ».

III.3.2 Une remise en ordre complexe, contrainte et controversée : moyens et enjeux d'un consensus multi-acteur

En ce vendredi 17 juin au matin, à la surprise répond l'urgence. Bloc d'enregistrement après bloc d'enregistrement, l'attaquant s'empare « de 258,056565⁴⁶⁰ ETH à la fois [, représentant] entre 3 500 et 5 550 dollars [, et ce] à peu près toutes les secondes, soit [...] entre 210 000 et 330 000 dollars par minute, ou entre 12,6 millions et 19,8 millions de dollars par heure » (Shin 2022, p. 149). La première alerte sur le Slack de « The DAO » permet à l'équipe de commencer à évaluer la situation, de relayer les premières informations et, surtout, de créer une cellule de crise avec les personnes clefs de l'écosystème. Car, dès le déclenchement, différentes stratégies de remédiation paraissent possibles, nécessitant des experts aux compétences différencierées. Outre l'option de ne rien faire (1), il est possible d'intervenir à la fois via le domaine applicatif et le domaine protocolaire : soit agir au sein de la lettre du code de « The DAO v.1 » (2, en Bleu, cf. section « Sauve-qui-peut » suivante) ; soit agir sur celle du protocole Ethereum lui-même, plus ou moins radicalement, par la publication d'une nouvelle version de l'implémentation protocolaire incluant un patch correctif soit de type *Soft Fork**, soit de type *Hard Fork** (3, en rouge, cf. section III.3.3 qui explicitera les deux formes), hiérarchiquement supérieur puisqu'il en contient les données endogènes* (Annexes n°V.6).

Figure 14: : Trois types de stratégies de remédiation



Source : Rolland Maël

⁴⁶⁰ L'attaquant a accumulé « 25 805,61 Tokens DAO (environ 4 650 \$) » dans l'adresse servant à l'attaque et la fonction split lui permet de réclamer des ETH au rapport de 100:1, d'où le drainage par transaction de 258,06 ETH (Shin 2022, p. 152).

Une cellule de crise à l'image des stratégies de remédiation : diversifiée

En premier lieu, Christoph avertit « *la Fondation Ethereum[,] Stephan et Griff* [sont choisis pour servir de] porte-voix [et] Simon, Lefteris et lui [tentent] de comprendre comment l'attaque [a] fonctionné et ce qui [peut] être fait » (*Ibid.*, p. 143). À Shangaï, V. Buterin, informé via Skype, pense d'abord à « spammer le réseau* pour ralentir l'attaque, pendant que lui et d'autres développeurs* essayaient de déterminer exactement ce qui se pass[e] » (Russo 2020, p. 188). Une cellule de crise (ou plutôt des cellules) excédant « Slock It » et regroupant des experts aux compétences différentes est rapidement constituée avec « *Christoph, Simon, Vitalik et les autres* [via la création de] groupes Skype [mais aussi Slack, etc. NDA] avec tous les anciens visages - Lefteris, Vitalik, Gav, Jeff, Aeron Buchanan, Péter Szilágyi, Christian Reitwießner, Avsa [Alex Van de Sande, NDA], Taylor Gerring, Fabian Vogelsteller, etc. » (Shin 2022, p. 144). V. Zamfir [Entretien n°9] prend part à cette cellule de « peut-être 10 à 20 [...] personnes dans ces canaux de discussion ». A « *l'époque [...] tout le monde était dans un état très réactif, [la] The Dao était drainé, et tout le monde regardait la page etherscan sans savoir ce qui se passait, [...] jusqu'à ce que nous découvrions [que] quelqu'un a trouvé le bug [...] et ensuite ce qui s'est passé en interne c'est que les gens ont dit hooo, que devrions-nous faire ?* » [Fabian Vogelsteller, Entretien n°12].

La crise « de vulnérabilité » concerne les codes de « The DAO v.1 » qu'exploite à son avantage un attaquant. La priorité est de cerner les mécanismes de l'attaques et le fonctionnement de « The DAO ». La compréhension des codes de « The DAO v.1 » est cruciale en ce qu'elle détermine les actions correctives possibles dans le cadre de « la lettre du code » de « The DAO ». Ces codes régissent toutes les procédures et délais d'intervention pour tous les participants, y compris l'attaquant. Cependant, les connaissances les entourant sont pour le moins asymétriques. L'attaquant est l'un des mieux informés. L'attaque « *n'est clairement pas triviale* » et la vulnérabilité était « *non seulement connue, mais corrigée par les créateurs [...] dans une mise à jour planifiée* [(la « The DAO v.1.1 »)] : mais alors qu'ils rédigeaient leurs articles de blog et criaient victoire, [voilà que] le pirate préparait et déployait un exploit ciblant [...] la fonction 'splitDAO' [dont il est le seul à avoir remarqué qu'elle] était vulnérable au modèle d'envoi récursif » (Daian 2016). À l'opposé, les membres de la cellule de crise « avaient différentes informations » et beaucoup de « questions » : qu'est « ce qu'il était possible de faire dans le software [,] comment fonctionne The DAO ? [...] Quels étaient les temps d'arrivée à différentes échéances ? Qu'est-ce qui pouvait se passer ? Qu'est-ce que pouvait faire le DAO Hacker ? À quel moment ? [V. Zamfir, Entretien n° 9]. La programmation complexe du fonds établit « *un jeu d'attente très compliqué. [...] Donc, il fallait arrêter [l'intervention de type Fork*] avant les échéances inscrites dans The DAO. Et il y avait beaucoup de controverses autour [des questions de] Fork*. Qu'est-ce que fait The DAO ? Où sont les différentes DAO ? Comment est-ce qu'on peut s'assurer qu'on les trouve et qu'on peut récupérer les fonds ? Et que le DAO Hacker n'obtienne pas de l'argent des DAO avant ça* » [V. Zamfir, Entretien n° 9]. Pour tout ce qui touchait à la programmation de « The DAO v.1 », « *seuls Christophe et Lefteris pouvaient répondre à ces questions* » [*Ibid.*] et « *ils ont essayé de discerner la méthode d'attaque pour pouvoir contre-attaquer et récupérer les pièces* » (Shin 2022, p. 144). La compréhension des codes de « The DAO » contraint la capacité des acteurs à mener des actions correctives au sein de la lettre des codes : les différentes échéances à tenir (le délai pour que les Ethers volés par l'attaquant deviennent transférables) s'imposant aux acteurs de la cellule pour que d'éventuelles actions correctives protocolaires soient décidées, mises en place et finalisées. Temps pour le moins restreint, que ce soit pour implémenter un patch correctif sous forme de *Fork** (*Soft* ou *Hard*), mais surtout pour le faire accepter par l'ensemble de la communauté alors qu'il est par nature plus controversé. Pour ce qui concerne le domaine protocolaire, « *seuls Gavin, Jeff et Vitalik pouvaient vraiment [agir] ... Moi et tout le monde on pouvait voir ce qui était possible sur le côté*

blockchain. Mais Gavin et Jeff devaient le faire. Leur équipe devait le faire. » [V. Zamfir, Entretien n° 9].

Le temps est au brainstorming, toutes les options de remédiation possibles doivent être proposées et évaluées. Dans « *un groupe Skype avec des opérateurs d'échange* », Buterin et d'autres discutent des « *stratégies de mitigation* » et celles auxquelles les opérateurs de bourses pourraient prendre part : « *saisir les fonds volés qui passeraient par des bourses d'échange* », comme ils le font généralement si d'aventure l'attaquant réussissait à les sortir de « *The DAO* » (*Ibid.*). À l'extrême et dans la panique, Buterin et George Hallam demandent la suspension des cotations ainsi que des dépôts et retraits d'Ether et de DAO Token : « *"TOUTES LES BOURSES : veuillez interrompre les échanges d'Ether dès que possible* » (George Hallam, porte-parole de la Fondation Ethereum cité par Russo 2020, p. 189). Présent, Dino Mark, co-auteur avec Sirer et Zamfir du « *Moratorium* », va jusqu'à aborder l'hypothèse d'un *Hard Fork** avec « *rollback* » : correspondant à un changement des règles protocolaires permettant un retour en arrière dans l'historique des enregistrements, cette éventualité est perçue comme violant le sacro-saint principe d'immutabilité (Shin 2022, p. 144). Les opérateurs de Bourse réagissent vivement à ce qu'ils considèrent comme des mesures radicales risquées : « *Tristan D'Agosta de Poloniex* » est critique, selon lui ce type de HF ne manquera « *de provoquer une panique sur le marché si la blockchain est considérée comme non fiable* », puisque soumise au désir de censure de certains. En outre, si certaines bourses acceptent d'arrêter le trading, d'autres se demandent « *si la mesure [est] absolument nécessaire* » car, pour autant que cela « *empêcherait l'attaquant de liquider des fonds, [cela] pénaliserait également les traders légitimes* » (Bill Shihara, CEO de Bittrex cité par Russo 2020, p. 189). Leurs clients traders, potentiellement investisseurs dans « *The DAO* », seraient pénalisés deux fois, par l'attaque et par cette mesure, les empêchant de quitter le marché au plus vite alors qu'ils anticipent, à raison, que le prix décrochera... Pour le coup, c'est un *vendredi noir* et le « *le jour de l'exploit, les détenteurs d'ETH et de DAO ont connu un véritable chaos [durant lequel] le prix de l'Ethereum a chuté de 21 dollars avant l'attaque à seulement 14 dollars après* » (Shin 2022, p. 153). Crack qu'on soupçonne d'avoir été exploité financièrement par l'attaquant, via une position vendeuse (*short*) puisqu'il en définissait la temporalité⁴⁶¹.

En quelques heures, par petits groupes et en secret, les membres des cellules ont entrevu différentes stratégies de remédiation possibles. Elles n'impliquent pas toutes ni les mêmes actions, ni les mêmes acteurs, ni les mêmes domaines d'intervention. Et il apparaît d'emblée que les actions sur le protocole de type *Fork** suscitent la controverse. Il est aussi temps d'informer le public des avancées en cours, de l'impliquer et d'évaluer sa réception des différentes solutions, dont les plus radicales nécessiteront l'implication de toutes les franges. Dans les deux heures de la découverte de l'attaque, Green informe la communauté « *The DAO* » via le « *Slack* » et « *DAOhub* » : « *@channel ALERTE D'URGENCE ! SI VOUS AVEZ UN SPLIT OUVERT, Veuillez ENVOYER UN MESSAGE À UN MEMBRE DE SLOCK.IT DÈS QUE POSSIBLE!!!* » (*Ibid.*, p. 143). Message repris et amplifié par Buterin répondant au billet de « *ledgerwatch* » sur Reddit par le même type d'appel : « *Il serait très utile que la personne dont le split se terminera dans 2 heures (#69) nous contacte.* » (Buterin 2016d). Ces premières réactions traduisent que des stratégies de contention sont à l'œuvre, marquant une nouvelle étape dans la remise en ordre. À 13 heures, Buterin (2016b)

⁴⁶¹ Des « *allégations [...] ont fait état d'un short Ethereum de 3 millions de dollars qui s'est produit sur Bitfinex quelques instants avant l'attaque, [...] clôturé avec un bénéfice de près de 1 million de dollars. [...] Tout attaquant motivé par des considérations financières [...] serait incité à s'assurer des profits, indépendamment d'un éventuel rollback ou fork, en vendant à découvert le jeton sous-jacent [car] la chute vertigineuse [du cours de l'Ether] qui s'est produite dans les minutes qui ont suivi le split malveillant offrait une excellente opportunité de profit [qu'] il aurait été stupide de ne pas saisir.* » (Daian 2016)

publie, via le Blog de la Fondation Ethereum, une « *mise à jour critique* » à l'adresse de la communauté Ethereum dans son ensemble. Le post est succinct et optimiste : l'annonce de l'attaque en cours précise déjà qu'il « *s'agit d'un problème qui affecte spécifiquement la DAO [et qu'] Ethereum lui-même est parfaitement sûr* », mais ajoute que, en tout état de cause, un « *Fork* logiciel a été proposé (sans ROLLBACK ; aucune transaction* ou bloc ne sera "inversé") qui [empêchera l'attaquant] de retirer l'Ether au-delà de la fenêtre de 27 jours.* » (*Ibid.*). Buterin tire même des événements des leçons pour le développement infrastructurel d'Ethereum, sous forme de conseils aux développeurs* : ils sont enjoins à prêter une grande attention aux « *bugs d'appels récursifs* », à se tenir informés « *des conseils de la communauté de programmation [et d'] éviter de créer des contrats qui contiennent plus de ~\$10m de valeur* »), tout en rappelant que des financements sont ouverts (« *DevGrants* », « *Blockchain Labs grants* » et « *String autonomous finance grants* ») à ceux travaillant sur « *les outils [...] qui facilitent l'écriture de contrats intelligents sûrs sur Ethereum* » (*Ibid.*). Voilà que vers « *13 heures, heure de Berlin, peu après la publication [de ce] billet de Vitalik, l'attaque de The DAO s'est arrêtée* », sans que l'on sache si le *smart contract** utilisé pour l'attaque a cessé de fonctionner (hypothèse de G. Green), ou si l'attaquant a pris peur des menaces brandies (hypothèse des autres membres de « *Slock It* » ; Shin 2022, p. 153).

50 nuances de « Code is Law » : un diagnostic et des stratégies de remédiation controversés

Nous l'avons vu, il n'y a pas de crise en soi et l'établissement d'un diagnostic de crise est un acte politique essentiel qui détermine, outre la « nature » de la pathologie (et sa gravité), le prescripteur, le malade, les traitements et le parcours de soin. Tout diagnostic de crise renvoie à une lecture imposée dans laquelle « *les problèmes publics résultent d'erreurs, de dysfonctionnements ou de mauvaise gestion* » servant non seulement à identifier les problèmes, mais aussi à légitimer les actions de différents acteurs en produisant du sens ou en contestant l'état du monde, et créant ainsi des fractures matérielles, idéelles et temporelles (Aguiton, Cabane et Cornilleau 2019, p. 10). Puisque « *mettre en crise, c'est [...] fabriquer un cadrage politique [permettant] soit de tracer des voies de "sortie de crise" [...], soit de construire des infrastructures de prévention en amont* » (Aguiton, Cabane et Cornilleau 2019, p. 15), c'est par définition une manière d'imputer et d'exonérer des responsabilités : « Quoi faire » sous-tend un « pourquoi », un « par qui » et un « à l'avantage / au désavantage de qui » ? Dans le cas de la crise Bitcoin CVE 2018, le bogue affecte les codes d'une implémentation logicielle protocolaire dont la maintenance est formellement à la charge d'une équipe. Le diagnostic du « bogue » et la voie de remédiation proposée font consensus entre tous, comme l'indique l'absence de controverse tant *a priori* entre les techniciens (au sein de l'arène locale du repo GitHub Bitcoin Core) qu'*a posteriori*, entre les autres composantes communautaires (après la publication du *post mortem*). C'est que la solution corrective (revenir à des codes antérieurs non vulnérables) est simple et n'ouvre aucun débat. Dans le cas de « The DAO », en ce vendredi 17 juin 2016, le concert des commentateurs s'étend sur la qualification d'« attaque », reconnaissant dans ce qui se passe l'existence d'un hiatus entre le résultat anticipé et celui effectivement obtenu du code de « The DAO v.1 » qui serait abusé par un acteur mal intentionné. Mais cette unanimité première va vite s'éroder, car la situation entourant la crise de « The DAO » est très différente.

Bien que le diagnostic considérant les faits comme une attaque liée à l'exploitation d'un bogue soit majoritairement partagé, une minorité va le contester. En second lieu, même en considérant la chose comme une attaque, les voies de remédiation sont multiples selon l'évaluation et les cadrages retenus de ces enjeux : « *Soft Fork*, Hard Fork*, contre-attaque, ne rien faire et de multiples combinaisons de ces options sont autant de voies possibles* » (Karapetsas 2016a). Les débats et dissensus entre spécialistes, apparus au sein de l'arène locale qu'est la cellule de crise, sont annonciateurs des débats publics. La présence de ces controverses conduit à mobiliser une

gouvernance publique dans la gestion de cette crise. Aucune solution n'est simple. Au-delà de questionner ce qui dysfonctionne, les diagnostics contradictoires réalisés et stratégies de remédiation proposées (cf. Figure 14 précédente) renvoient à l'hétérogénéité des risques perçus (pour la communauté « The DAO » ou pour Ethereum dans son entier), à des coûts et bénéfices associés à chacune des stratégies offertes (coûts économiques auxquels s'en ajoutent d'autres, en termes d'image et de motivation communautaire) enfin, à l'assignation de responsabilités *via* la définition de statuts et rôles pour chacun des acteurs dans cette remise en ordre. Pour chaque voie de remédiation, la question de sa légitimité communautaire fait débat : se dessinent, concernant la « bonne » gouvernance d'Ethereum, des positions oscillant entre les deux pôles idéal-typiques déjà posés (cf. Chap. II section II.3.3). Certains réduisent cette légitimité à une simple question de conformité des actions aux principes du "Code is Law" dans sa version la plus rigoriste et hypostasiée (cf. l'idéal-type de la « loi de Szabo ») : tout résultat de code est par définition légitime, la déférence au code (Hinkes 2021) et à l'*« autorité algorithmique »* (Lustig et Nardi 2015), même fautive, doit être totale. Face à ces représentations de *coiners**, d'autres positions existent et vont s'imposer (plus proches du pôle idéal-typique opposé de la « Loi Crypto » de Zamfir 2019). Ce cas démontre l'hétérogénéité de vues monétaires structurant ces communautés, leur évolutivité*, donc le fait qu'*« autorité algorithmique »* et *« déférence au code »* sont complétées d'une gouvernance humaine et sociale essentielle. On retrouve les conclusions du chapitre II : pour nous, la qualité et la viabilité d'une CM, comme la confiance/défiance qui en sous-tendent les usages, s'apprécient à l'aune de sa capacité à se reproduire légitimement aux yeux des acteurs. D'où l'intérêt d'étudier une crise à gouvernance *publique* qui, contrairement au cas du huis clos, voit s'exprimer un dissensus éclairant plus crûment les rapports, attentes et désirs pluriels qu'ont les *coiners** envers leur système de paiement et l'*« autorité algorithmique »* (Lustig et Nardi 2015) qu'ils lui accordent.

La figure précédente (Figure 14) distingue trois types de stratégies de remédiation suivant le rapport qu'entretiennent leur justification à l'interprétation rigoriste du « *Code is Law* » et à l'*« autorité algorithmique »* pleine qui devrait en découler. Elles ne relèvent ni du même cadrage politique, ni des mêmes domaines d'intervention, ni des même acteurs. Et leur efficacité est incertaine. D'un côté, les actions agissant, comme l'attaquant, *au sein* de la lettre des codes (1 et 2, en Bleu, présentés dans la section « *Sauve-qui-peut* » suivante) : ces interventions sont par nature limitées à contenir et minimiser les pertes financières auxquelles les membres de « The DAO » font face. Le second type est théoriquement plus efficace, permettant une remise en ordre globale en agissant directement « sur » la lettre du code protocolaire d'Ethereum (et donc sur les données endogènes* hiérarchiquement inférieures, cf. Annexe n°V.6). Mais, à son efficacité théorique répond son caractère incertain, lent et politiquement complexe. Ce type d'intervention suppose des modifications protocolaires radicales (3, en rouge, cf. section III.3.3), qui dépendent « *de la communauté Ethereum au sens large pour [leur] mise en œuvre* » (Karapetsas 2016b). À travers la présentation des enjeux de ces familles d'intervention (plus individuels ou collectifs), de leurs cadrages et des débats qu'ils vont susciter, il est permis de comprendre les ressorts de cette crise ouverte à gouvernance publique. La légitimité, accordée ou non à chaque famille d'intervention, renverra aux questionnements communautaires sur les propriétés désirées de leur CM et de la « bonne » gouvernance qui y est associée.

« *Ne rien faire* » (1)

Partant de l'interprétation rigoriste du « *Code Is Law* », certains arguent que l'attaquant n'est qu'un usager agissant dans les limites définies par le code. Dans ce cadre, il n'y a pas d'attaque et il est légitime de ne rien faire. Pour les tenants de cette vision, impossible d'être *coiners** sans se revendiquer du camp de la règle radicalisée, où la seule « bonne » gouvernance préservant les propriétés qu'ils attendent d'Ethereum est que les équipes de développement, tant de « Slock It »

que d'Ethereum, n'agissent pas. La controverse se structure autour de ce qui est conçu au sein de l'interprétation rigoriste du « *Code Is Law* » comme deux paradoxes (Xiangfu Zhao et al. 2017, p. 3) déjà en partie soulignés (cf. section III.2.1) : à considérer la « lettre du code » comme toujours légitime, les actions de l'attaquant sont « légales » au sens de « *The DAOv.1* » ; dans ces conditions, pourquoi les qualifier d'attaques ? Le second paradoxe touche au principe d'immutabilité au cœur de ces représentations libérales-technicistes : les modifications protocolaires annoncées contreviendraient à cette propriété hypostasiée, donc à l'« esprit du code », au même titre que les actions de l'attaquant. Des arguments de ce type sont mobilisés par certains pour s'opposer vocalement à tout type d'intervention, comme le 18 juin, où un des opposants, travesti en un attaquant auto-proclamé (dont la « *signature fantaisiste* » échoue à prouver cette identité, Buterin 2016) publie une « *lettre ouverte* » adressée à « *The DAO et à la communauté Ethereum* » où des arguments similaires assoient des menaces d'actions juridiques (Attaquant auto-proclamé 2016).

Cette « *lettre ouverte* » pointe que « *Slock It* » devrait s'en tenir aux conditions d'utilisation encadrant l'ICO stipulant leur absence de responsabilité⁴⁶². Et ce, en cohérence avec l'inscription du projet dans ce type d'interprétation rigoriste du « *Code is Law* », qui a alimenté la perception d'un projet radicalement innovant et l'euphorie entourant son ICO. Des représentations libérales-technicistes sont revendiquées, tant par le projet « *Slock It* » que par ses membres, et se trouvent au fondement du design des mécanismes de gouvernance de « *The DAO* ». Dès l'origine, les références à la « *loi de Szabo* » (et au travaux de Nick Szabo) sont explicites (Jentzsch 2016b, p. 1). Les principes de conception déjà entrevus renvoient à « *un modèle de comportement humain [...] basé sur des idéologies libérales, où les humains agissent comme des agents rationnels, intéressés et sans confiance* » (DuPont 2018, p. 12). De ces fondements est née l'idée d'un fonds d'investissement vendu comme devant forcément être plus efficace car « *dirigé par un code informatique immuable, par opposition [aux] règlements fragiles et complexes* » entre entités centralisées (Tual 2016e). L'équipe de conception⁴⁶³ et la communauté en formation y font extensivement référence. Pour beaucoup, l'intérêt fut suscité parce qu'avec « *The DAO* », « *non seulement [il] avait le code is law en pratique mais aussi dans le contrat, dans le contrat il y avait un élément qui disait[:] si jamais il y a une différence entre la description du système [l'esprit du code pour nous, NDA] et son fonctionnement effectif [la lettre du code, NDA] c'est le smart contract** [donc la lettre défaillante du code] qui prime. » [C. Lesage, Entretien n°22]. En conséquence, le fait que l'entité numérique attaquée soit immuable et indépendante est à l'origine une propriété, non un bogue. Des choix idéologiques ont conduit à ce qu'aucun garde-fou sécuritaire (coupe-circuit, privilège, mise à jour, etc.) ne soit implémenté, autre qu'un processus de migration, long et à quorum de participation élevé, permettant si nécessaire aux investisseurs de migrer d'une instance de *smart contract** à une autre contenant des mises à jour⁴⁶⁴. C'est cette même procédure

⁴⁶² L'« *Avis de non-responsabilité* » (« *Disclaimer* ») stipule que, sans pouvoir « *spéculer sur le statut juridique des DAO dans le monde* », reste que « *toute personne qui utilise le cadre générique de la DAO, y compris la DAO appelée "La DAO" ou toute autre DAO, le fait à ses propres risques [et] les auteurs ne sont pas un cabinet d'avocats, [ils] n'ont pas vocation à offrir des conseils juridiques [aussi, si] vous créez une DAO, ce sera votre DAO et vous serez responsable de son fonctionnement* ». Voir <https://github.com/blockchainsllc/DAO/blob/develop/README.md> [consultation au 12/06/2021].

⁴⁶³ Certains membres de l'équipe, comme G. Green, ne cachent pas leur libertarianisme : à l'époque de sa découverte de Bitcoin, il était « *très opposé à la Réserve fédérale, au système bancaire, j'étais un mordu de l'or, vous savez, le type de gars libertarien classique et euh. Je mettais tout mon argent dans l'or et l'argent et j'ai entendu parler de cette histoire de Bitcoin* » (THE FILTER 2016). Souhaitant « *jouer le marché libre sans les gouvernements et les banques* » (*Ibid.*), il se retrouve dans la vision portée par « *The DAO* » : « *c'est le rêve du Réseau de partage universel [...] un réseau ouvert sans permission qui va permettre une véritable économie de partage* » (Griff Green and the DAO | Layer Zero 2021).

⁴⁶⁴ L'existence de ce processus de mise à jour est un gage contre toute forme d'action discrétionnaire, permettant tout à la fois à « *The DAO de maintenir un code statique immuable sur la blockchain* Ethereum, tout en étant capable d'être mis à jour si le besoin s'en fait sentir* », voir Jentzsch 2016b.

que devait emprunter la nouvelle version corrigée (« The DAO v.1.1 »), qui en l'état ne sert à rien. Puisque « *ce contrat fera toujours exactement ce pour quoi il est programmé et ne pourra pas être abusé* » (Jentzsch 2016b), il faudra faire avec les codes fautifs : « The DAO » est sans commandement, ni moyen de se défendre, puisqu'aucun individu ou groupe, pas même l'équipe de développement, ne dispose de priviléges exorbitants en son sein. Tous ces arguments sont mobilisés par l'attaquant auto-proclamé (2016). Il dit avoir participé à l'ICO après avoir « *examiné attentivement le code de la DAO [et] découvert la fonction qui permet de récompenser le split par de l'éther supplémentaire* [, fonction qu'il a utilisée afin de] *réclam[er] à juste titre 3 641 694 ethers*. *[Il est] déçu par ceux qui qualifient de "vol" l'utilisation de cette fonctionnalité intentionnelle* [car il] *utilise cette fonctionnalité explicitement codée selon les termes du contrat intelligent** [et son] *cabinet d'avocats* [confirmerait que son usage est] *entièrement conforme au droit pénal et délictuel des États-Unis*. À titre de référence, veuillez consulter les conditions de la DAO : "Les conditions de la création de la DAO sont énoncées dans le code du contrat intelligent* existant sur la blockchain Ethereum à 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Rien dans cette explication des termes ou dans tout autre document ou communication ne peut modifier ou ajouter des obligations ou des garanties supplémentaires au-delà de celles énoncées dans le code de la DAO. Tous les termes ou descriptions explicatifs sont simplement offerts à des fins éducatives et ne remplacent ni ne modifient les termes explicites du code de la DAO énoncés sur la blockchain ; dans la mesure où vous pensez qu'il y a un conflit ou une divergence entre les descriptions offertes ici et la fonctionnalité du code de la DAO à 0xbb9bc244d798123fde783fcc1c72d3bb8c1894, le code de la DAO contrôle et définit tous les termes de la création de la DAO. » (Attaquant auto-proclamé 2016)

Quant à intervenir sur les codes d'Ethereum, la situation est claire : Ethereum n'est pour rien dans l'attaque, il « *a fonctionné exactement comme prévu* » (@IAMnotA_Cylon cité par Shin 2022, p. 156). Aussi, de prime abord, au sein du « *canal interne à la Fondation* [Ethereum, NDA] [...] il y avait beaucoup d'opinions différentes [et selon] la plupart des gens [...] nous ne devrions rien faire, ce n'[était] pas notre problème... » [Fabian Vogelsteller, Entretien n°12]. Puisqu'il s'agit « *simplement d'une exploitation du code logiciel que chaque investisseur de la DAO avait accepté* » (Walch 2017b, p. 17), et qu'Ethereum - ses codes protocolaires et finalement ses équipes de développement - ne sont pas responsables (comme le précise d'emblée l'annonce de Buterin), pourquoi agir ? En outre, compte tenu de la responsabilité individuelle souveraine des investisseurs qui n'ont pas fait leur propre recherche et qui n'auraient pas dû faire confiance (cf. « *Do Your Own Research* » / « *Don't trust, verify* »), il était justifié de « *laisser brûler The DAO* ». Cela servirait de leçon coûteuse dans la « *vie réelle* » (« G. T. Blossom », 2016, cité par DuPont, 2008, p. 11). Il fallait choisir ce que la crise « The DAO » allait incarner : « *Un Soft ou Hard Fork* équivaudrait à la saisie de[s] éthers légitimes* [de l'attaquant], *réclamés légalement selon les termes d'un contrat intelligent** [et] *ruinerait de façon permanente et irrévocable toute confiance non seulement dans Ethereum mais aussi dans le domaine des contrats intelligents et de la technologie blockchain*. *De nombreux grands détenteurs d'Ethereum se débarrasseront de leur argent, et les développeurs*, les chercheurs et les entreprises quitteront Ethereum* [car] *toute fourche, qu'elle soit douce ou dure, nuira [...] à Ethereum et détruira sa réputation et son attrait*. [L'attaquant conclut qu'il se] *réserve le droit d'intenter toute action en justice contre les complices du vol, du gel ou de la saisie illégitime de mon éther légitime, et je travaille activement avec mon cabinet d'avocats*. [...] J'espère que cet événement sera une expérience enrichissante pour la communauté Ethereum et je vous souhaite bonne chance. Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées » (Attaquant auto-proclamé 2016).

Au sein de la Fondation Ethereum une majorité est ballotée entre l'inaction ou l'absence d'opinions claires, mais pour une petite minorité l'inaction n'est pas envisageable.

« Sauve-qui-peut » au sein de « la lettre du code »

Certains ne peuvent se rallier aux arguments du camp précédent. De leur point de vue, cette crise et ses conséquences excèdent largement « The DAO » et sa communauté du fait du contexte : Ethereum n'en est qu'à ces balbutiements et cette crise pourrait se révéler coûteuse, voire mortelle, pour un jeune écosystème qui commence sa phase de « preuve de concept ». La petite taille de la communauté est une contrainte, et la part importante d'Ether volée par l'attaquant pose des questions économiques, réputationnelles, mais aussi juridiques. En contexte de grande incertitude réglementaire, cela pouvait conduire à ce que « *les codeurs d'Ethereum et de la DAO [soient l'objet de] poursuites judiciaires* » et, plus généralement, à créer un « *œil noir pour la technologie* » Ethereum (Walch 2017b, p. 17) : la somme « *volée représentait plus de trois pour cent de tout l'éther, ce qui aurait eu un impact négatif sur l'ensemble de l'espace et [sur] la motivation des développeurs* qui construisent sur Ethereum [car] en même temps, tout était plus petit. [...] Si nous laissons maintenant cette chose, c'est foutu, [...] nous devons faire quelque chose, [...] imaginez que vous ayez une maison en feu et qu'il y a cent personnes debout devant... et qu'une seule décide d'entrer et d'aider le bébé ou les gens à l'intérieur...* » [Fabian Vogelsteller, Entretien n°12]. La petitesse d'Ethereum qui le met en péril devient alors une ressource en termes de coordination : « *C'était un très petit écosystème [,] tout le monde était sur le subreddit de Reddit [,] tous les développeurs* et presque tous les projets [déployés sur Ethereum, NdA], il n'y en avait que 50 ou 100 [et] vous pouviez essentiellement connaître tout le monde [,] 200 personnes ou quelque chose comme ça [...]. Vous pouvez juste parler directement à tout le monde de tout parce que c'était juste minuscule* » [B. Summerwill, Entretien n° 26].

Ces arguments convainquent certaines figures de la communauté qu'il faut « *agir, ce n'est qu'un MVP⁴⁶⁵ tout ceci n'est qu'un début, la communauté est suffisamment petite, nous pouvons résoudre le problème, pourquoi [ne] pas le faire ?* » [Fabian Vogelsteller, Entretien n°12].

« Se sauver soi-même au détriment des autres » (2-b)

Contrairement aux arguments précédents, retenir la version la plus rigoriste du « *Code is Law* » n'impose pas l'inaction. Si ce qu'a fait l'attaquant est légitime, tout usager peut faire de même vis-à-vis de « The DAO » ou de la DAO enfant de l'attaquant. Les tenants de cette interprétation s'opposent à ceux qui voient en l'inaction la seule fin désirable justifiant qu'il est possible de ne pas remettre en cause la propriété d'immutabilité tout en intervenant (comme l'attaquant) dans le cadre strict de « la lettre des codes ». Au sein des stratégies de « sauve-qui-peut », certaines relèvent de simples stratégies palliatives et visent à atténuer individuellement les conséquences de l'attaque (2-b). Ces actions correctives impliquent une mise en œuvre brouillonne, non coordonnée et non coopérative.

Spammer le réseau* Ethereum (2-a) permet de gagner du temps, mais en même temps que cela ralentit l'attaque, cela complique pour tout le monde les interactions *on chain**. Bien que l'attaque ait pris fin, elle apparaît comme une « divulgation non responsable », qui risque d'entraîner des imitations (cf. Figure 9 ci-dessus), d'autant que des publications explicitent les mécanismes de l'attaque (Daian 2016 ; Gün Sirer 2016) : la survenue d'*« attaques par imitation »* devient *« la principale inquiétude »*, car il devient facile de « *s'inspirer de cette attaque et la reproduire à l'identique* » (Gün Sirer 2016). Ces attaques d'imitation ne manqueront pas d'avvenir d'ailleurs les jours suivants (Campbell 2016). Face à l'urgence, il est temps d'agir et la première stratégie au sein

⁴⁶⁵ Pour « Produit minimum viable » (« *Minimal Viable Product* ») qui, dans le cadre de la conception produit, renvoie à une des premières versions mises en production afin de récolter les premiers retours utilisateurs.

des codes accessibles aux acteurs individuellement est non coopérative et sous-optimale. Elle correspond, pour les porteurs de DAO Tokens, à utiliser la fonction Split pour créer une DAO enfant en vue de récupérer les fonds investis au taux défini initialement. Chaque porteur peut initier la procédure de création d'une DAO enfant via la fonction Split qu'a utilisée l'attaquant, s'il est suffisamment compétent pour suivre la procédure explicitée sur Reddit. L'équipe du portefeuille non intermédiaire « MyEtherWallet » a en effet développé un outil simplifiant le split pour baisser les barrières à l'entrée technique (Monahan 2016 ; FelixA 2016b) Clément Lesaege [Entretien n°22] est de ces techniciens compétents (cf. biographie Annexe n°IV.4) : « *Pour moi, à l'époque, le premier impératif, c'était surtout d'essayer de récupérer les Ethers que j'avais mis dedans. [...] J'avais compris [...] qu'il y avait deux solutions [:] récupérer notre stake [ou] attaquer l'attaquant* ». Il opte « *pour Fork*er une DAO enfant [, il a] fait [s]on proposal de Fork*ing [, et lorsqu'il] est arrivé à expiration [il] étais[t] maintenant à un point où [il] pouvait [...] transformer les DAO tokens en Ether au bon taux* » [Ibid.]. Cependant, c'est une stratégie non coopérative à somme nulle. La récupération des fonds par ceux qui l'entreprennent accroît des pertes pour les autres restant dans l'entité originelle « The DAO » : « *au bout d'un moment, le DAO aurait été insolvable. Si tout le monde fait ça, ça ne marchait pas* » [Ibid.]. C. Lesaege finira par « *décid[er] de ne pas utiliser ces Fork*ing proposals* » : déjà, car il « *avai[t] peur de ce qui risquerait de se passer au sein de la DAO enfant* », ensuite, il voulait « *éviter de splitter les communautés* », enfin et surtout, il était devenu clair qu'« *Ethereum allait bien être Fork*é* » [Ibid.].

Une deuxième solution qui consiste à attaquer l'attaquant suppose une intervention coordonnée selon une logique collective, visant à rendre difficile, voire impossible, à l'attaquant de bénéficier des fonds volés (2-c et d). Cette action devait permettre l'ouverture éventuelle de négociations en vue de la restitution totale ou partielle des fonds (2- e): « *pour ça, on aurait eu besoin de faire un vote du DAO [,] on ne pouvait pas juste le faire tout seul. Donc, l'idée, c'était de s'organiser et de créer une sorte d'équipe pour faire ça, que j'ai d'abord essayé de faire. Mais rapidement, j'ai trouvé des personnes [proches de] The DAO, le White Hat Group [à cette époque il s'agit encore du « Robin Hood Group », NdA], qui étaient déjà un peu plus avancées. On en a parlé un peu.* » [Clément Lesaege, Entretien n°22]

« *Contre-attaquer : action collective et coordonnée en vue d'un intérêt commun* » (2 – c, d, e)

À l'origine, la plupart des acteurs se revendiquent du camp de la moindre intervention, mais face à la crise, des premiers désistements de « *Curators* » arrivent, comme celui de « *Gavin* [, qui] a été le premier [suivi par] de plus en plus de gens [abandonnant] parce qu'ils pensaient que c'était trop risqué, [certains ont] ressenti [que] quelqu'un devait faire quelque chose sinon, rien ne se serait passé. » [Fabian Vogelsteller, Entretien n°12] Des membres de la cellule de crise se constituent en un groupe de *Pirates* à « *Chapeau Blanc* » (« *White Hat Group* » ou WHG ; Campbell 2016 ; Karapetsas 2016b ; Bitmex Research 2017b ; Muratov et Vogelsteller 2016). Ce premier groupe, qui se recomposera au gré des évènements à venir, est nommé le « *Robin Hood Group* » [:] « *ce n'était pas seulement* [Fabian Vogelsteller], *c'était Alex* [Van de Sande, qui propose le nom comme une plaisanterie, Entretien n°13], *c'était Jordy* [Baylina], *c'était Griff* [Green] » (pour ceux publiquement identifiés RHG ci-après, cf. Tableau 10 suivant) et ils se sont « *dit ok faisons quelque chose* » [Fabian Vogelsteller, Entretien n°12]. Ces acteurs (identifiés ou non) précisent que cette intervention « *n'est pas officielle [,] il s'agit d'une action collective menée par des individus qui ne représentent aucun de leurs employeurs* » (Van de Sande 2016a). La contre-attaque est constituée de deux volets distincts jouant sur le fait que « *l'attaque [...] fonctionnait dans les deux sens* » : l'exploitation de la même vulnérabilité de réentrance doit permettre, d'un côté, de « *sécuriser* » les fonds restants encore susceptibles d'être volés et, d'un autre côté, de « *hacker en retour* » la DAO enfant de l'attaquant [V. Zamfir, Entretien n° 9] afin de l'empêcher de récupérer les gains

escomptés, avec en ligne de mire : la poursuite de « *négociations [...] avec l'attaquant ou [la survenue d'un] Fork** » (2-e; Karapetsas 2016d).

Ces opérations opèrent dans le cadre du « *Code is Law* », prenant l'attaquant à son propre jeu. On trouve les justifications de cette riposte dans l'annonce faite par « *Slock it* » (*Ibid.*). Le premier volet de l'intervention s'adresse aux « *détenteurs de jetons DAO* » qui voudraient agir « *au cas où le Soft Fork* ne serait pas mis en œuvre* » (*Ibid.*) : dans l'éventualité où il ne serait « *pas implémenté, la communauté [The DAO reste en capacité d']empêcher l'attaquant de retirer ses ETH, même après l'expiration de la période de 27 jours, en [rejoignant sa DAO enfant]. Cette solution n'est pas complète et n'aboutira probablement jamais à la restitution de l'ether volé aux DTH d'origine, mais elle empêchera au moins l'attaquant de percevoir des bénéfices.* » (*Ibid.*). L'annonce précise que cette intervention a peu chance d'aboutir, « *le timing est essentiel* », la communauté *The DAO* n'a que « *25 jours avant que la phase de création de la DAO enfant de l'attaquant ne se termine* » (*Ibid.*) et, d'ici là, un ensemble d'actions devra être réalisé (*Ibid.*). C'est encore par exploitation de la vulnérabilité de réentrance qu'est entrepris le deuxième volet, qui correspond à un sauvetage des fonds encore vulnérables : la contre-attaque du RHG, lancée dans le secret le 20 juin, sera rendue publique le 21 juin (Karapetsas 2016b ; FelixA 2016a ; Muratov et Vogelsteller 2016 ; Campbell 2016) : « *THE DAO EST EN TRAIN D'ÊTRE DRAINÉ EN TOUTE SÉCURITÉ. NE PANIQUEZ PAS.* » (Van de Sande 2016⁴⁶⁶) Cette opération prend la forme de « *deux siphonnages [...] effectués sur la DAO [permettant qu'] un total de 7 630 479 ETH [soit] placé dans des DAOs enfants [...] actuellement sous contrôle (principalement) ami* » (Karapetsas 2016b ; Buterin 2016a ; Shin 2022, p. 143). Le RHG promet : « *dès que cette DAO aura atteint sa maturité, nous essaierons de transférer tous les fonds dans un contrat de remboursement* » (A. Van de Sande, cité par Campbell 2016) permettant à leur propriétaire légitime (les porteurs de DAO Tokens) de les réclamer. La situation est stabilisée pour un temps seulement. Si les ETH sont « *en sécurité pour le moment* », « *un Soft Fork* ou un Hard Fork* est nécessaire pour les sécuriser pleinement* » (Karapetsas 2016b). La vulnérabilité reste présente dans tous les codes des DAO enfants créés, « *les fonds [sont] en danger indéfiniment [:] la répétabilité de l'attaque par réentrance dans les deux sens* » fait craindre à l'équipe une « *guerre de DAO* » : que l'attaquant riposte, imposant encore d'agir et que « *la situation [dure] éternellement* » (C. Jentzsch, cité par David Z. Morris 2023). L'attaquant leur donne raison. Le 22 est annoncé qu'il a donné « *de l'éther à la DAO et [rejoint ainsi] l'un des splits whitehat* », mais la communauté est enjointe à ne pas « *paniquer* », « *tout autre mouvement que l'attaquant essaierait de faire se produirait après 24 jours* », « *cela [...] donne plus de temps qu'il n'en faut pour mettre en place un Fork** » (Karapetsas 2016c).

⁴⁶⁶ Voir <https://x.com/avsa/status/745313647514226688>, un usager lui répond : « RIEN NE DIT MIEUX "NE PAS PANIQUER" QUE LES MAJUSCULES » (voir <https://x.com/KyleRiecker/status/745343956528037888>, repris par (Russo 2020, p. 200)).

Tableau 10 : Les différents acteurs de la contre-attaque

Organisations	Action(s) entreprise(s)	Nom et prénom
« Robin Hood Group » ou RHG (1 ^{er} groupe)	Mise en œuvre d'une stratégie de sécurisation des fonds et de contre-attaques	Baylina Jordi
		Green Griff
		Karaptetsas Lefteris
		Alex Van de Sande
		Vogelsteller Fabian
« White Hat Group » ou WHG (2 ^{ème} groupe, cf. section suivante.)	Mise en œuvre de la restitution des fonds sauvegardés	Baylina Jordi
		Green Griff
		Karaptetsas Lefteris
Entreprise « Bity »	Facilitation des opérations des deux groupes : - Représentation et conseil juridique - Aide à la sécurisation et à la conversion des fonds sous contrôle (Vente <i>via</i> les comptes de Bity)	Bochsler Gian
		Roussel Alexis

Source : Rolland Maël

Le drainage des fonds de « The DAO », deuxième volet de la contre-attaque, marque la fin de ce qui n'est que la première phase du sauvetage, celle du « Robin Hood Group ». À ce point, tous les acteurs attendent la survenue d'un *Fork** (et certains y travaillent) pour régler définitivement la crise. Et tous postulent (et soutiennent l'idée) qu'un *Soft Fork** suffira. Ils se trompent, un *Hard Fork** sera finalement nécessaire, d'où un piratage blanc décomposé en deux temps : « *avant et après le Fork** ». Ainsi, le WHG ne réapparaîtra que tardivement, après le HF et le maintien-surprise de l'ancienne chaîne.

III.3.3 Gouvernance ouverte et publique pour des *Forks* controversés

Les voies de remédiation précédentes sont difficilement critiquables du point de vue rigoriste du « *Code is Law* » car, que l'on reconnaissse ou non les faits comme relevant d'une attaque illégitime, elles sont effectuées légitimement dans le cadre de la « lettre » des codes. Mais, de ce fait, leur efficacité est relativement faible : partielles, elles se limitent à réduire les pertes et non à recouvrer les fonds volés. Sur les deux volets de la contre-attaque, seul le second est un succès : près de 70% des ETH dans « The DAO.v1 » sont contrôlés. Parallèlement et dès le déclenchement de l'attaque, les acteurs savent (Zamfir l'avait même anticipé⁴⁶⁷) qu'une remédiation totale est à portée *via* la dernière famille de stratégies : « Fork*er », c'est-à-dire faire évoluer radicalement les règles protocolaires, hiérarchiquement supérieures aux règles de « The DAO.v1 » contenues dans sa couche base de données (cf. Annexe n° V.6) pour régler la situation. À l'efficacité de ces modifications répond un encadrement et des contraintes de coordination communautaire élevées, du fait d'attendus renforcés en termes de discussion, de publicité, de quorum.

« *To Fork or not to Fork* »⁴⁶⁸ : enjeux et controverses théoriques autour des *Forks*

Les stratégies consistant à intervenir directement sur la lettre du code d'Ethereum sont considérées comme radicales et, de ce fait, sont controversées. Pour toute communauté *coineuse*, ce type de modification est considéré comme « critique » en ce qu'elles touchent aux règles consensuellement acceptées librement par l'ensemble des usagers (ici les *etheristes*). Le cas de crise précédent à mis au jour, pour Bitcoin, l'institutionnalisation de la procédure particulière des « *Bitcoin Improvement Proposal* » (BIP) encadrant ces modifications (cf. section III.2.1). La plupart des communautés de CM reprennent à Bitcoin cette procédure formelle en l'adaptant ; Ethereum n'y dérogera pas avec la procédure des « *Ethereum Improvement Proposal* » (ou EIP). Mais, en ce début de phase de « preuve de concept », cette dernière manque encore. Dans le jargon des *coiners**, ces évolutions sont aussi qualifiées de *Fork**, car elles impliquent de « *copier un programme [logiciel] existant et d'en distribuer une version modifiée* » (Nyman2015, p. 1 ; cité par Walch, Kuo et Deng 2017, p. 14) selon la pratique de bifurcation de code au sein des répertoires des forges logicielles, qui permet de créer une nouvelle version ou un nouveau logiciel indépendant (si les droits accordés le permettent). À la faveur d'un processus de normalisation commencé par les *bitcoiners** (autour de la classification et de l'encadrement des BIP justement, voir Andresen 2012 ; Timón 2015 ; Lombrozo 2015 ; Lombrozo 2017) et poursuivi par des *etheristes* (Buterin 2017c), ces *Forks** se répartissent en deux grands types : les *Soft Forks** et les *Hard Forks**.

Un *Soft Fork** correspond à toute modification qui réduit strictement le nombre de transactions* valides au sein de l'ancien protocole, là où un *Hard Fork** rend valides des transactions* et des enregistrements qui ne l'étaient pas dans l'ancien protocole (Buterin 2017c). En conséquence, dans le cadre d'un *Soft Fork**, les nœuds* qui suivent les anciennes règles restent compatibles avec le protocole de registre* distribué, « *de sorte que tous ceux qui ont déjà le même logiciel peuvent en principe le valider dans la mesure où ils le peuvent, [...] personne n'est lésé, les règles sont essentiellement les mêmes* » [J. Song, Entretien n°14]. Bien qu'une majorité de nœuds*

⁴⁶⁷ Vlad Zamfir, dans son opposition théorique à la loi de Szabo et en affirmation de sa « loi crypto », a toujours milité pour que les modifications protocolaire soient de type *Hard Fork*, car elles objectivent la dimension socio-politique de la gouvernance des CM. Depuis ce positionnement, il poste sur Twitter/X dès le 14 mai 2016 le message mi-sérieux, mi-provocateur suivant : « *la communauté ferait-elle un Hard Fork d'Ethereum s'il y avait un bug critique dans le DAO ? :p* » (Zamfir 2016) ; à quoi on lui répond : « *Je me demandais la même chose. Ça ne va pas être joli. :(* » (de la Rouvière 2016)

⁴⁶⁸ Titre d'un billet de blog de Polrot (2016a) du 27 juin 2016, pour Ethereum France ; et de Jeffrey Wilcke publié pour la Fondation Ethereum, le 15 juillet 2016.

doit se mettre à jour pour rendre exécutoires les nouvelles règles, leur qualité de rétrocompatibilité font que les contraintes de coordination et de coercition sont faibles : « *les Soft Fork* sont plus pratiques pour les utilisateurs, car [ils] n'ont pas besoin d'effectuer une mise à jour pour rester sur la chaîne* [, ils] sont moins susceptibles de conduire à une scission de la chaîne [et] ne requièrent réellement que le consentement des mineurs/validateurs » (Buterin 2017c). À l'inverse, bien que les *Hard Forks** « *offrent aux développeurs* beaucoup plus de souplesse dans la mise à jour du protocole, car ils n'ont pas à veiller à ce que les nouvelles règles “s'intègrent” dans les anciennes règles* », les contraintes de coordination et de coercition sont fortes : ils « *requièrent le consentement des utilisateurs (opt-in)* » et tous sont dans l'obligation de se mettre à jour, sans quoi ceux opérant des nœuds* obsolètes, dorénavant non compatibles, participeront d'un protocole de registre* distribué et d'une CM distincts suivant des règles de consensus différentes de la majorité (Buterin 2017c). Cette coercition, les *bitcoiners** disent la rejeter. Ce type d'évolution n'est rien que « *le lancement d'une nouvelle pièce, parce que cela n'est pas rétrocompatible, vous commencez quelque chose de nouveau* [...] *on peut ajouter de nouvelles pièces, on peut en éliminer d'autres, on peut modifier le calendrier d'approvisionnement, on peut faire n'importe quoi.* [...] *Quand vous avez quelque chose comme Ethereum qui HF de temps en temps, ils peuvent changer les règles* [...] *cela signifie que s'ils le veulent, ils ne le feront sûrement pas, mais s'ils le veulent, ils pourraient dire, ok, le gouvernement de la Russie peut obtenir cent millions d'Ethereum et ainsi de suite* » [J. Song, Entretien n°14]. Ceci explique chez eux une préférence pour les *Soft Forks** rétrocompatibles, gages d'une souveraineté hors coercition : tout *bitcoiner* conservait tout à la fois la possibilité de ne pas accepter les mises à jour et la possibilité de participer au consensus de son nœud. Cependant, cette affirmation participe davantage d'une mise en récit. Bien qu'on « *entend souvent dire que l'on peut utiliser la toute première version du logiciel Bitcoin et qu'elle sera compatible avec le réseau** actuel [...] *la véritable réponse est beaucoup plus compliquée et nuancée* » ; certaines modifications délicates seront nécessaires et le résultat incertain (Lopp 2022). En outre, l'histoire de Bitcoin permet de questionner la rétrocompatibilité effective de certains *Soft Forks**⁴⁶⁹ comme de reconnaître que Bitcoin aussi a connu des *Hard Forks**, des *rollbacks* même considérant que des historiques longs de dizaines de blocs ont été rendus orphelins. Ce fut le cas de la crise « *Bitcoin bug Value Overflow* », administrée centralement par Nakamoto et dont la mise à jour, n'en déplaise à Song, forçait les opérateurs de nœuds* (mineurs ou complets) à remplacer leurs versions locales du registre* pour revenir à une version précédente choisie à sa discrédition (cf. section III.I.2). Ou celle dite « *CVE 2013 #3220* » (crises n° 4 et n°19 de notre Chronologie n°3), que Dino Mark mobilise contre les critiques des *Hard Forks** de Tristan d'Agosta de Poloniex : « *c'est ce qui s'est passé avec le bitcoin en 2013. Les bourses ont annulé les transactions** » consécutivement à la scission de chaîne (Shin 2022, p. 144).

Ce cadre qui fait des *Soft Forks** l'outil privilégié de la gouvernance des codes protocolaires d'une CM est celui qui accueille les controverses suscitées par la question d'un *Fork** pour remédier à la crise en cours. Le premier chapitre a montré comment Ethereum, influencé par la culture des *bitcoiners** de 2014, se distingue de manière critique de Bitcoin. Cela ne doit pas faire oublier des continuités. Au commencement, Ethereum et sa communauté empruntent pour partie aux *bitcoiners** le fond libéral-techniciste présenté. L'inscription du projet « *The DAO* » dans l'ethos du « *Code Is Law* » et son succès l'illustrent de manière exemplaire. C'est la survenue d'imprévus qui va imposer la solution d'un *Hard Fork**, que bien peu d'*etheristes* soutiennent de prime abord. Pour le comprendre, rappelons-nous que, dès la conception d'Ethereum, l'évolution du protocole par *Fork** (potentiellement *Hard*) est théorisée et même souhaitée (cf. « *difficulty bomb* », Chap. I section I.3.3) : cela s'inscrit dans un principe d'agilité visant à être moins rigide au niveau infrastructurel que Bitcoin. Pour autant, un *Fork**, et tout particulièrement un « *hard Fork** est [...]

⁴⁶⁹ Certains *coiners* pointent en particulier SEgwit.

un sujet très controversé et, pour de bonnes raisons, [il ne doit] être qu'une solution de dernier recours » (Jentzsch 2016c). D'autres principes doivent guider la prise de décision : simplicité, universalité, modularité et, bien sûr, la réaffirmation d'un principe de non-discrimination et de résistance à la censure*... assurant que les évolutions d'Ethereum ne servent pas à restreindre ou empêcher des catégories spécifiques d'usages et d'usagers, ou à s'opposer à des applications considérées par certains comme indésirables. Pour ceux qui considèrent que ce vol ne pose de problème qu'à « The DAO » et à sa communauté, les *Forks** entrevus, *Soft* ou *Hard*, semblent contrevenir à ces principes. Cette situation éclaire l'embarras provoqué dans la communauté Ethereum et les critiques émanant de l'extérieur, particulièrement des *bitcoiners**. Pour nombre de *coiners**, le HF n'est légitime ni dans son fond, ni dans sa forme. Dans le fond, « *le hack de DAO [est singulièrement] différent* », [car avec ce] *hard Fork**, *ce n'est pas la compatibilité avec la version précédente qui est en cause, c'[est] essentiellement un renflouement pour les gens qui ont fait un investissement dans DAO, qui s'est avéré avoir une faille [afin de] s'assurer que 16% de tout l'Ether qui était dans le DAO Hack ne soit pas drainé.* » [J. Song, Entretien n°14]. Leur conclusion sur la forme est tout aussi définitive. Corallo affirme qu'avec « *le DAO Hack [...] c'est un cercle étroit de développeurs* qui [aurait] décidé qu'il y avait une sorte de communauté [, mais] la priorité absolue n'était pas la communauté décide [, c']était prenons une décision et espérons que nous pourrons impliquer la communauté partout où nous le pourrons* » [Entretien n°15]. Phuc de généraliser : pour lui, « *sur Ethereum, quand tu as besoin d'un correctif d'urgence [...] ben les développeurs*, ils prennent l'initiative ils développent le truc [...] ils vont appeler les différents clients quoi et puis cela sera appliqué le lendemain il n'y aura pas de discussion en général. [...] On leur pose moins de questions que chez Bitcoin* », ce qui démontrerait leur « *pouvoir [...] d'influencer le code dans une direction ou dans une autre.* » [M. Phuc, Entretien n° 19]. Les *bitcoiners** considèrent ainsi que la gouvernance de cette crise relève de l'imposition par le haut de modifications protocolaires à tous les utilisateurs, par un pouvoir centralisé et technocratique gisant dans la main des « Core Devs » d'Ethereum.

Pourtant, cette crise d'« évolution » implique, à la manière de celle rencontrée par Bitcoin, une gouvernance ouverte polycéphale, mobilisant des acteurs de nos différents domaines infrastructurels (cf. Chap. I section I.2). Aux enjeux de légitimité des modifications s'ajoutent des contraintes de coordination élevées. Ces mêmes groupes devront participer aux prochaines étapes de la production d'un consensus, qui s'avère de fait complexe et problématique, car, quoiqu'en disent les *bitcoiners**, Ethereum repose sur une multiplicité d'implémentations clients, donc autant d'équipes de « Core Devs » indépendantes, qui doivent dès lors s'entendre et coopérer, dans la production d'un *Fork** que la communauté devra valider.

La production d'un *Fork* : processus incertain, multi-acteur et multiniveau

Intervenir sur la lettre des codes protocolaires n'est pas du même ordre qu'agir au sein des codes. Toute la communauté Ethereum est de fait impliquée dans la résolution, pas seulement la partie (même importante) des participants à « The DAO ». L'implémentation d'un *Fork** - *Soft* ou *Hard*, est un processus hors de portée de la communauté « The Dao » et de l'équipe « Slock It », justifiant en parallèle les attaques en « Chapeau Blanc » au cas où il n'aboutirait pas. La création d'un correctif repose sur les équipes de développement des implémentations logicielles d'Ethereum, et s'appuie sur le même type de maintenance que celle évoquée pour Bitcoin. Cette maintenance, avec quelques différences, repose sur les mêmes types d'acteurs (les « Core Devs »), de dispositifs socio-techniques (des « *repo Github* ») et de procédures d'encadrement. Les *Forks** de « The DAO » n'ont pas suivi la procédure des IEP censée encadrer les modifications protocolaires radicales, puisqu'elle n'était pas encore institutionnalisée. C'est cette résolution qui en posera les bases, à partir des dispositifs et procédures *ad hoc* mis en place afin d'assurer au *Fork** une

légitimité communautaire maximale. Cette famille d'interventions nous place dans une crise d'« évolution » à gouvernance publique (donc dans un cadre proche de la procédure des BIP synthétisée en Figure 13). La controverse ouverte immédiatement au déclenchement de la crise montre que la reconnaissance d'une transgression de la lettre des codes d'Ethereum à leur esprit n'est pas évidente pour la communauté. Diagnostics et solutions ne sont pas confinés aux « Core Devs » d'Ethereum, mais relèvent d'un problème public et de négociations communautaires ouvertes en urgence. La production d'information, les arènes de débats et la formation d'évaluations partagées (en débats) excèdent, dès le début, le cercle des développeurs* et vont même au-delà de la cellule de crise. Cette dimension globale se reflète aussi dans les profils des participants aux discussions préliminaires desdites cellules de crise, qui couvrent l'ensemble des groupes de parties prenantes de la gouvernance d'une CM, que nous avons déjà cernés : médias et chercheurs, développeurs* (couches applicative et protocolaire), utilisateurs finaux, mineurs et assimilés, services marchands et passerelles*. Contrairement à la gouvernance de « huis clos » et sans être à l'époque formellement encadré, il apparaît d'emblée que le consensus se doit d'être global et non local. Les équipes de « Core Devs » sont d'abord réticentes, considérant qu'il n'est pas de leur ressort d'influencer un tel choix communautaire : le *Soft Fork** et le *Hard Fork** discutés par la communauté seront produits en parallèle, les *etheristes* trancheront. La participation des composantes communautaires dans les débats et décisions s'est réalisée au travers d'une variété de médias et d'arènes de discussion, ainsi que d'une pluralité de dispositifs de mesure du consentement (*on chain** et *off chain**) pour impliquer au-delà du cercle des opérateurs du traitement des transactions*.

Dans les débats initiaux, un *Soft Fork** est privilégié par les protagonistes. Si un *Hard Fork** représente pour Tual, comme pour d'autres, « *la voie la plus simple, la plus rapide et la plus sûre* », pour la majorité il est « *l'option nucléaire* ». Le risque est trop grand « *de diviser la communauté* » alors que le *Soft Fork** annoncé suffit à limiter la perte à « *30% [ce qui apparaît] parfaitement acceptable* » (Shin 2022, p. 165). Ce *Soft Fork**, annoncé par V. Buterin (2016) le 17 juin, doit encore être spécifié, implémenté dans des codes protocolaires et publié avant de passer l'épreuve de la légitimité communautaire. Dans le cas d'Ethereum, ces activités vont mobiliser, non quelques membres d'une équipe unique de développement, mais différents types de contributeurs plus ou moins intégrés dans des équipes de développement différenciées. La « *spécification initiale a été réalisée [...] par Christophe Jentsz* [, qui] *avait le plus grand intérêt à faire disparaître ce problème* [qui entachait] *sa réputation personnelle et son travail* [: il] *demandait à tout le monde [de] faire quelque chose [...] et il [fut] celui qui a [coordonné l']équipe sur la spécification* » [Fabian Vogelsteller, Entretien n°12]. La spécification du *Soft Fork** seul ne suffit pas, il faut encore la traduire en code protocolaire. Mais voilà, si Bitcoin est structuré autour de l'implémentation hégémonique « *Bitcoin Core* », vendue comme garante d'une meilleure stabilité du protocole, les *etheristes* y voient une centralisation risquée : « *le problème que vous avez [, c'] est que le Core client de Bitcoin, c'est le standard. [...] C'est comme si Bitcoin est décentralisé, mais il ne l'est pas* » puisque vous n'avez qu'un « *groupe de développeurs** principaux [qui] vont décider de ce qui se passe. » [B. Summer Hill, Entretien n°26]. Ethereum a choisi *a contrario* d'*« avoir des clients multiples* » et donc différentes équipes avec différents intérêts et points de vue [B. Summerwill, Entretien n°26, cf. Tableau 11 suivant]. Avant même le lancement d'Ethereum coexistait une diversité d'implémentations protocolaires indépendantes, avec « *Vitalik qui faisait un client Python, Gav qui faisait un client C++, Jeff qui faisait un client en Go, tout en parallèle* » [B. Summerwill, Entretien n° 26]⁴⁷⁰. Cette diversité s'explique parce qu'il est « *plus facile de faire un client Ethereum qu'un client Bitcoin* », car Ethereum, lui, « *est complètement spécifié. On a le Yellow Paper qui*

⁴⁷⁰ Quatre clients sont développés avant la *presale* : « *l'intention était de n'avoir que trois implémentations [, et] un membre de la communauté [...] a indépendamment proposé un client Java.* » (Buterin 2014c; Buterin 2014g)

explique toutes les spécifications » [S. Polrot, Entretien n°16]. À partir de ces spécifications, tout développeur* peut rédiger une implémentation logicielle dans le langage de programmation* de son choix : là où « *Bitcoin Core c'est [...] nul n'entre ici s'il ne fait du C++ [,] le positionnement d'Ethereum est plus universaliste. [...] Le Yellow Paper [...] décrit spécifiquement comment chaque fonction doit être implémentée, comment elles doivent se comporter et ce qu'elles doivent donner. Et donc, si on suit le Yellow Paper pour créer un logiciel, bah normalement, il est rétrocompatible avec le reste. [...] Ce qui [...] invite beaucoup de gens à s'intéresser au cœur du truc* » [de Tychet, Entretien n° 4].

Tableau 11 : Ethereum, un réseau constitué d'implémentations diversifiées

Implémentation client	Part du réseau*	Implémentation client	Part du réseau*
Geth <i>(+ Gexp)</i>	97,44% <i>(94,89% +2,55%)</i>	Geth	79,52%
Parity	1,45%	Openethereum. (ex Parity) ⁴⁷¹	5,76%
Autres (<1%) <i>(CPP Ethereum/Aleth ; Gshif)</i>	1,09% <i>(0,11%+0.98%)</i>	<i>Implémentations dépréciées</i> <i>(CPP/Aleth le 06/10/2021 ;</i>	
		Erigon	9.34%
		Hyperledger / Besu	2.92%
		Nethermind	2.05%
		Autres (<0.2%) <i>(trippynode; coregeth; teth; akula; bor; ethlightnode; merp-client; bitcoind)</i>	< 1 %

Sources : Rolland Maël, Données
<https://web.archive.org/web/20160718202836/http://ethernodes.org/network/1> [consultation au 09/06/2022], traitement de l'auteur.

Pour les *etheristes*, il est « très positif » qu'Ethereum dispose d'« énormément de clients » écrits dans une pluralité de langages de programmation⁴⁷² [S. Polrot, Entretien n°16] : en plus de permettre une meilleure résilience du réseau* (en cas de faille dans une implémentation, les autres restent disponibles), cela accroît le nombre et la diversité des profils participant de la gouvernance des codes protocolaires. Et ces développeurs* trouvent plus facilement que sur Bitcoin à être financés. Dès l'origine, ils peuvent compter sur la Fondation Ethereum, qui doit amorcer le

⁴⁷¹ Le cas *Parity* est symptomatique du phénomène de turn-over : il est développé par les équipes d'*EthCore*, l'entreprise de Gavin Wood, qui l'abandonne le 02/06/2020 pour se consacrer au développement d'un protocole concurrent d'Ethereum, *PolkaDot*. *Ethcore* a « transféré la base de code *Parity Ethereum* vers une DAO composée de développeurs* et d'organisations » (*Parity Technologies* 2019). *Parity* devient alors « *OpenEthereum* », définitivement abandonnée en juillet 2021. (<https://ethereum.org/ka/deprecated-software/> [consultation au 09/06/2022]).

⁴⁷² Outre « *Parity, qui est écrit en Rust et Geth qui est écrit en Go, il y a CPP Ethereum qui est un client C++, il y a Trinity, qui est un client en Python, il y a PyEthereum qui est écrit en Python aussi, Panthéon/Pegasys que je citais tout à l'heure qui est écrit en Java, donc il y en a une multitude quoi. Il y a même un Ethereum H en Haskell.* » [J. De Tychet, Entretien n°4]

développement du protocole et, plus généralement, de son écosystème (Buterin 2014c ; Buterin 2014j). C'est la Fondation Ethereum qui, par ses statuts, doit favoriser cette diversité (Ethereum Foundation 2021)⁴⁷³. À l'époque, disposant des ressources tirées de la *presale*, elle finance en propre des développeurs* et chercheurs (en freelance, comme V. Zamfir, Entretien n°9), mais aussi des équipes indépendantes, reposant sur des entités juridiques hétérogènes : « *vous avez la Fondation Ethereum [...] mais l'équipe de développement réelle était sous une entité légale différente, appelée EthDev [...] à Berlin, l'entité juridique était différente de celle de Londres, et [aussi] de celle en Hollande. L'équipe Gav se trouvait à Amsterdam [et aussi] à Berlin [où] elle s'occupait du client C++, mais aussi des tests.* [B. Summerwill, Entretien n°26]. En outre, toutes les implémentations Ethereum n'ont pas la même importance dans la structuration du réseau*, surtout à l'époque de « *The DAO* ». Comme pour Bitcoin, une implémentation jouit d'un statut de référent : « *Geth* » écrit en GO, choisie par près de 97,5% des opérateurs de noeuds*. Là encore, le statut d'implémentation « *focale* » relève moins d'une assignation formelle que d'une convention d'acteurs⁴⁷⁴ : Geth est le client officiel de l'EF, sa maintenance n'a jamais été remise en cause, contrastant avec le turn-over des implémentations indépendantes (turn-over dénoté en grisé, cf. Tableau 11, ci-dessus⁴⁷⁵) et a *de facto* tenu le rôle de « *client de référence, [car il est] écrit normalement de la façon la plus lisible possible* » [S. Polrot, Entretien n°16]. À ces avantages répond un inconvénient : il est nécessaire de maintenir une parfaite compatibilité protocolaire entre des logiciels indépendants reposant sur « *des piles technologiques presque entièrement différentes entre l'équipe C++ et l'équipe GO* », par exemple [B. Summerwill, Entretien n° 26]. Alors, « *évidemment, il va y avoir des petits trucs, des petits machins, il va falloir aller regarder comment* » chaque équipe code les spécifications, « *par exemple, le python et le C++* » [J De Tychet, Entretien n° 4]. Cette « *triangulation entre la spécification et les implémentations de la spécification* » fait de l'interopérabilité un enjeu central de la sécurité d'Ethereum : « *est-ce que les clients peuvent se parler entre eux ?* » [B. Summerwill, Entretien n° 26] Cette capacité des implémentations à communiquer entre elles dépend de la capacité de coordination et de coopération des équipes, qui sont elles-mêmes soumises à des aléas personnels, mais aussi organisationnels⁴⁷⁶.

⁴⁷³ Pour une présentation exhaustive des actions menées par l'EF, voir <https://ethereum.org/en/foundation/> [consultation au 13/06/2022] ou le premier rapport financier (Ethereum Foundation 2022).

⁴⁷⁴ Cette position peut changer, « *maintenant je crois que le client de référence, c'est considéré comme étant le client Python. Parce que c'est plus lisible. Et il est aussi maintenu par la Fondation le client Python [.] Les personnes qui souhaitent développer leurs clients se basent plutôt sur la version Python de la Fondation.* » [S. Polrot, Entretien n°16] Ce statut implique des efforts particuliers pour les équipes de maintenance qui en ont la charge, en termes de clarté d'écriture payée au prix d'une moindre efficience : « *La référence, ça a été Go très longtemps, aujourd'hui Python et du coup Go a plutôt switché sur une implémentation d'exécution. Et c'était devenu nécessaire parce que, comme Parity a depuis le début été une implémentation focus performance, il commençait à y avoir une différence de performance assez forte entre les deux. Et donc Geth avait du mal à suivre Parity* » [S. Polrot Entretien n°16].

⁴⁷⁵ Pour Geth, voir <https://geth.ethereum.org/>; concernant les clients dépréciés, voir <https://ethereum.org/ka/deprecated-software/> [consultation au 09/06/2022].

⁴⁷⁶ B. Summerwill [Entretien n° 26] décrit comment la question de la coordination recouvre différents problèmes imbriqués : « *On m'a dit des choses sur, tu sais, sur Charles [Hoskinson, l'un des co-fondateurs exclus, cf. Chap. I section I.3.2] qui est un mauvais gars et [...] et ho Gav est égoïste et [...] vous savez, vous héritez [...] des préjugés du groupe dans lequel vous êtes [et d'un autre côté] il y avait beaucoup de vitriol et de haine ou quoi que ce soit envers la fondation [.] Entre l'équipe C++ et l'équipe GO [...] c'est comme si [elles] ne pouvaient même pas se parler. Vous avez aussi "Mist" le navigateur [dont l'équipe et celle] de Gav travaillent bien ensemble, mais vous avez comme Forteresse qui encombre la zone de Gav et vous avez cette compétition bizarre entre la Fondation et Ethdev, comme si la Fondation gardait l'argent, comme si c'était la volonté de Vitalik. Ensuite vous avez l'équipe de développement qui construit les clients. Mais il s'agissait en fait d'entités juridiques à but lucratif. EthDev UG, qui se trouve à Berlin et qui existe toujours, était [...] la société à but lucratif de Gav, [...] il y avait aussi une entité juridique à Londres. C'était un vrai bazar avec tout ce tas d'entités juridiques et il y avait à l'origine une séparation entre la Fondation, qui fournissait l'argent, et les sociétés qui s'occupaient du développement. La concurrence s'est accrue au fil du temps.* »

Les développeurs* de l'implémentation GO Ethereum s'emparent des spécifications de Jentsch pour les traduire en un *Soft Fork** : « *Peter Szilagyi, [...] le bras droit de Jeff Wilcke dans l'équipe Go Ethereum, dirigeait les efforts pour [...] le client Geth* » (Russo 2020, p. 203 ; Entretien n°12). Les correctifs sont publiés le 24 juin, pour Geth (v. 1.4.8) et Parity (v 1.2.0), accompagnés d'un billet de blog de Szilàgyi (2016) intitulé « DAO Wars : Votre voix sur le dilemme du soft-Fork* ». À partir du constat selon lequel il « *n'y a pas de ligne de conduite claire et optimale qui satisferait tous les membres de la communauté de manière égale, [il a été décidé] de donner le pouvoir aux personnes qui gèrent Ethereum de décider s'ils soutiennent cette décision ou non* ». Les versions patchées bloquent au niveau protocolaire le compte de l'attaquant, ainsi « *la communauté [pourra décider] de geler les fonds* » via l'établissement d'une « *liste blanche* » dont est exclue l'adresse de l'attaquant (*Ibid.*) : sera ignoré « *tout bloc contenant une transaction* qui aide l'attaquant à déplacer les fonds de la Dark DAO [...,] fonds [dès lors] éliminés du système, et [seuls ceux] du White Hat Group pourront être restitués aux investisseurs de la DAO, à raison de 0,70 ether pour chaque ether investi* » (Gün Sirer, Keefer et Hess 2016). Chaque utilisateur doit décider s'il soutient l'activation du *Fork**. Télécharger le logiciel patché ne suffit pas, il faut exprimer son accord *via* une procédure de vote par signalement qui conduira, ou non, à son activation : ceux qui s'y opposent peuvent, au choix, ne pas se mettre à jour ou lancer les nouvelles versions en mode par défaut sans signalement⁴⁷⁷.

Malgré un soutien important, notamment des mineurs, publicisé sur les forums et via des billets de blogs (au sein des *pools* importantes, qui ont mis en place des outils de suivi de la « *distribution des votes* », comme Dwarfpool, Ethermine, Ethpool, le consensus est favorable au *Soft Fork** à près de 80%, FelixA 2016a), cette procédure ne parviendra jamais à son terme. Le 28 juin, Gun Sirer et d'autres annoncent publiquement que le remède est pire que le mal : le correctif introduit « *un vecteur d'attaque par déni de service* » au sein d'Ethereum⁴⁷⁸.

Arènes et dispositifs d'expression du désaccord : le camp du *Hard Fork rallié par la majorité**

Avec l'abandon forcé du *Soft Fork**, la possibilité d'une intervention peu invasive s'effondre alors que la fenêtre d'opportunités, elle, se réduit. L'attaquant sera bientôt en capacité d'accéder aux fonds volés. Le *Hard Fork**, bien qu'impopulaire, s'érige en solution de dernier ressort, et les débats houleux reprennent de plus belle. En outre, par précaution, le développement du *Hard Fork** a été réalisé en parallèle de celui du *Soft Fork**, avec les mêmes acteurs à la manœuvre (Wilcke 2016 ; V. Zamfir, Entretien n° 9) : « *Christophe ne savait pas quoi faire [...] il est allé voir la seule personne qui aurait pu les aider à faire quelque chose à propos du Hard Fork*. Et il a demandé à Jeffrey Wilcke [, qui de prime abord] ne voulait pas du tout faire partie de ça, il s'en fichait. Mais en même temps, il était le seul qui pouvait construire un Hard Fork* dans ce court laps de temps* » [Fabian Vogelsteller, Entretien n°12]. Reste un double défi dans le temps impari : convaincre

⁴⁷⁷ « *Les mineurs supportant le DAO Soft Fork peuvent le faire en démarrant Geth 1.4.8 avec --dao-soft-fork. Cela aura pour effet d'abaisser les limites de gaz des blocs vers Pi million jusqu'à ce que le bloc décisif 1800000 (environ 6 jours à partir de maintenant) soit atteint. Si la limite de gaz de ce bloc est inférieure ou égale à 4M, le Soft Fork entre en vigueur et (toutes les mises à jour) les mineurs commenceront à bloquer les transactions DAO qui libèrent des fonds. Les mineurs qui ne supportent pas le Soft Fork DAO peuvent exécuter Geth normalement sans avoir besoin d'arguments supplémentaires. Ils essaieront de maintenir les limites de gaz des blocs à leur niveau actuel de 4,7 millions. Si la limite de gaz du bloc décisif est supérieure à 4 millions, le Soft Fork est refusé et les mineurs (tous ceux qui se mettent à jour) acceptent les transactions DAO qui libèrent des fonds.* » (Szilàgyi 2016)

⁴⁷⁸ Avec les nouvelles règles implémentées, « *un attaquant peut alimenter le réseau avec des transactions qui exécutent des calculs complexes et se terminent par une opération sur le contrat DAO. Les mineurs utilisant le Soft Fork se verraien contraints d'exécuter, puis d'abandonner, de tels contrats sans percevoir aucune rémunération.* » (Gün Sirer, Keefer et Hess, 2016)

l'autre camp du bien-fondé de sa position et mesurer les avis communautaires exprimés. Dans les débats, très majoritairement publics, le camp de l'intervention s'affermi. Pour lui, « *la Blockchain est immuable jusqu'à ce qu'on décide qu'elle ne le soit plus* », tout le « *problème, [...] c'est qui ce "on" et comment on prend la décision ? [...] Si on veut bouger les choses, ben il faut un peu faire la démonstration qu'on a la population derrière, en tout cas l'opinion publique.* » [S.Polrot, Entretien n°16]. L'évaluation de l'assentiment communautaire est constitutif des débats autour des Forks*. Là où, sur Bitcoin, les procédures de type vote/signalement ont été privilégiées, ne donnant la voix qu'aux seuls mineurs (et à leurs intérêts potentiellement opposés à ceux des autres composantes communautaires), la communauté Ethereum vise à définir exhaustivement ses parties prenantes pour leur donner la parole : « *ça a été tout l'objet du débat, les signaux, la recherche de signaux pour essayer de comprendre, ce que la Communauté voulait en fait. Je me souviens des heures passées à essayer de comprendre [...] quelle était la qualité, la valeur des différents signaux : il y avait les posts sur « Reddit », [...] Crypto- Twitter [...]. Il y avait par contre les votes des mineurs déjà, des pools de minage.[...] Et puis le fameux « Coin Vote », enfin « Carbon vote ». Après, il y avait tous les signaux de gens d'autorité, on va dire.* » [S. Polrot, Entretien n°16]. Aucune solution unique n'apparaît satisfaisante. D'où l'émergence d'une pluralité de dispositifs, à l'initiative de la Fondation Ethereum ou d'*etheristes* plus anonymes.

Afin de saisir la communauté dans toutes ses composantes, ces solutions se répartissent entre des dispositifs de type *on chain**, considérés comme plus « objectifs » et d'autres *off chain**, plus « subjectifs », dont la complémentarité apparaît essentielle pour une gouvernance équilibrée. Il est tout d'abord nécessaire de donner la parole aux opérateurs du traitement des transactions* : ce sont eux qui, en dernière instance, rendent exécutoires les règles protocolaires, anciennes ou nouvelles. Leur voix est facile à récolter et objectivement vérifiable : la PoW* protège des attaques sybilles, et les parts relatives de puissance de calcul pointant en faveur ou contre la mise à jour ne peuvent être truquées : « *chaque personne qui participait à la pool de minage pouvait signaler s'il était pour ou contre le Fork*, et donc il y avait des tableaux mis à jour en temps réel, par des gens de la communauté, c'était assez bien fait. Qui là penchait plus vers le Fork** » [S. Polrot, Entretien n° 16]. Mais le périmètre de la communauté Ethereum ne se réduit pas à ces opérateurs qualifiés. Si tous ne souhaitent pas gérer les contraintes d'une mise à jour de noeuds* dans un écosystème balbutiant (la démarche n'était pas si ardue, nous l'avons nous-même effectuée), cela ne veut pas dire qu'ils revendiquent le silence. Tout porteur d'Ether est par définition membre de la communauté de paiement. Des dispositifs *on chain** peuvent permettre une mesure « objective » avec des dispositifs de « *coinvote* », permettant de voter dans un sens ou dans l'autre avec ses ETH. La Fondation, qui développait un dispositif de ce type, fut coiffée sur le poteau par une solution alternative, « *Carbon Vote [...] un site Web mis en place par des Chinois, où vous pouviez voter avec la quantité d'ether* » [Fabian Vogelsteller, Entretien n°12]. Pour y prendre part, « *il fallait aller chercher son cold wallet, faire une transaction* et dire je vote [...], le coup d'opportunité pour voter [était] assez énorme, il [fallait] se déplacer avec des clés qui sont [...] critiques pour voter et plus tu as un solde important d'Ether, plus tu vas avoir un poids important dans le carbon vote. Plus tu as un solde important d'Ether, plus tu as intérêt d'avoir un cold wallet et de les y mettre.* » [J. de Tychet, Entretien n° 4]. Ces contraintes expliquent que nous n'ayons pas voté nous-même alors que le résultat, qui n'allait pas changer substantiellement, nous convenait [cf. Annexes n°IV.1]. Bien que considérés comme plus objectifs, ces dispositifs de « *gouvernance on chain** » apparaissaient incapables de représenter l'ensemble des intérêts présents dans la communauté, et il fut considéré que se limiter à eux serait vecteur d'affaiblissement, dessinant un système « *ploutocratique* » au profit des seuls mineurs et gros porteurs (Zamfir 2017). Pour donner la parole à des franges communautaires silencierées par ces dispositifs, les *etheristes*, de manière plus ou moins coordonnée, ont innové et mis en place un éventail de solutions *off chain** : ouvertes à tous et plus faciles d'accès, elles sont cependant sujettes à caution, puisque non protégées des attaques sybilles et tentatives de fraude. En l'espèce, des

dispositifs de sondage sur des plateformes dédiées (comme sur change.org dès le 20 juin, réunissant 1 061 signataires), mais aussi les réseaux* sociaux comme Reddit et Twitter, les forums de Slock It, de The DAO, etc. ont été mis en œuvre.

Ces différents dispositifs de mesure ont fait ressortir rapidement qu'une majorité importante de la communauté se rallie à l'idée du *Hard Fork**, qui était condamnée de prime abord. En première ligne, les « Core Devs » qui ne voulaient pas apparaître comme ceux imposant par le haut un tel changement : le Carbon Vote est déterminant, quand « *50% de tous les ethers ont voté à 80% en faveur du Hard Fork** [,] ça a été un signal clair pour Jeffrey : "OK, il y a une demande et je dois faire quelque chose, parce que je suis le seul à faire quelque chose". » [Fabian Vogelsteller, Entretien n°12]. Nombreux sont ceux dont les positions ont évolué au gré des débats : « *Ma première réaction a été non, bien sûr, vous ne devriez pas bifurquer. Et puis il y a eu ce mois de débat le plus intense, sur ce qu'on va faire ? [...] Je suppose que je suis venu pour les voir, vous savez, la valeur des deux côtés. [...] Il y avait des mérites des deux côtés. Et c'était en gros comme, écoutez, vous savez, la majorité des gens sont pour le Hard Fork**. » [B. Summerwill, Entretien n° 26]. Les figures d'influence, « *rapidement [Vitalik, Gavin, etc.] se sont mis d'accord, autour du fait de faire le Fork**. Et d'autant plus après l'arrêt du Soft Fork* [...], sur tous les canaux, tous les gens que je considérais, [...] comme des gens d'autorité étaient pour le Hard Fork** aussi. » [S. Polrot, Entretien n° 16]. Les conditions d'activation renvoient à des choix d'arrangements socio-techniques différents, selon les équipes de développement. Pour Geth, ce sont les résultats de « *l'outil communautaire carbon vote* [qui seront] utilisés pour définir l'option de Fork* par défaut » (*Ibid.*). Du côté du client Mist, les développeurs* décident, pour plus de neutralité, de ne « *donner aucun choix prédéfini, [mais une] fenêtre [demande explicitement] aux gens d'appuyer sur "Yes Fork"** ou "*No Fork**" [: sur] environ 8 000 nœuds*, [...] 7 900 étaient le navigateur Mist, donc les gens ont choisi [Il rigole]. C'était très clairement extrêmement démocratique... [À l'inverse de] ces théories du complot comme quoi la Fondation était impliquée dans The DAO et essayait de s'aider elle-même et tout ça, c'est des conneries. » [Fabian Vogelsteller, Entretien n° 12 ; nous-mêmes, utilisateur de ce client, avons dû effectuer ce choix].

III.3.4 « Fork You ?! » : une scission surprise fondatrice et ses enseignements

Des résultats des débats et dispositifs d'expression du consensus / des désaccords variés mis en œuvre, il semble à tous que le *Hard Fork** est acquis et à une écrasante majorité. Les voix *anti-Forks**, en plus d'être largement minoritaires, semblent « *bizarres* », « *la moitié des gens qui postaient on les avait jamais vus avant [...] c'était assez louche, ce qui se passait sur Reddit* » contre le *Fork** [S. Polrot, Entretien n°16]. À tous niveaux, « *on avait une assez écrasante majorité, il me semble 98% et quelques, qui votait pour la Fork** [au niveau des nœuds* mineurs se signalant, NDA]. Et ensuite les échanges se sont prononcés en disant ben nous on suivra la chaîne principale... et le jour de la Fork*, il y avait 97% du hash*rate qui pointait vers la chaîne Fork*ée et 3% vers Ethereum non Fork*ée et très rapidement on est tombé à 100% » [J. de Tychet, Entretien n° 4]. Dans ces conditions, tous attendent une simple mise à jour qui conduirait à ce que l'ensemble des nœuds* rejoigne les nouvelles règles protocolaires. Aucun n'anticipe encore que certains acteurs continueront d'appliquer les anciennes règles, revendiquant de maintenir une chaîne minoritaire en vie et, à travers elle, la vision originale d'Ethereum.

Un *Hard Fork* et ses attendus théoriques

Le 20 juillet, l'heure est à la célébration : « *quel accomplissement !* » pour Jentzsch (2016a), quand Buterin (2016a) félicite « *la communauté Ethereum pour la réussite du hard Fork** ». Après un signalement majoritaire, l'activation du *Hard Fork** s'est déroulée comme programmé. Par jeux d'écritures, il doit permettre de renvoyer à un passé qui n'a jamais eu de réalité au sein de la chaîne

Ethereum, toutes les interactions réalisées avec le contrat « The DAO v.1 » depuis la conclusion de l'ICO (donc celles liées à l'attaque) et de recouvrer ses fonds dans des contrats de réclamation : « *The DAO [...], son extraBalance [...], tous les enfants [...] et l'extraBalance de chaque enfant sont encodés dans une liste L au bloc 1880000 [et au] début du bloc [...] 1920000 [...] tout l'ether de tous les comptes de la liste L sera transféré vers le compte de contrat* » (Wilcke 2016). Avec son activation est exécuté le « *changement d'état irrégulier qui [transfert] ~12 millions d'ETH des contrats "Dark DAO" et "Whitehat DAO" vers le contrat de récupération WithdrawDAO* », duquel « *les détenteurs de jetons DAO peuvent [réclamer leur] ETH à un taux de 1 ETH = 100 DAO* » (*Ibid.*). Le Hard Fork* ne touche qu'au smart contract* de « The DAO ». « *Ce n'est pas la même chose que si vous faites un hard Fork* sur Bitcoin, [car] si vous voulez changer une transaction* passée, vous devez faire un rollback et ce sont toutes les transactions* qui se produisent après qui sont affectées. Sur Ethereum, [du fait d'un] modèle basé sur le compte, vous pouvez seulement toucher The DAO sans toucher l'argent de quelqu'un d'autre [, donc] le seul impact négatif [...] c'est que maintenant l'algorithme de consensus* a un morceau de code supplémentaire qui dit, dans un bloc de 3 millions, faites ceci au lieu de cela* » [Fabian Vogelsteller, Entretien n°12].

Du fait de cette majorité forte en faveur du Hard Fork*, tous anticipent le même futur proche. Il est de connaissance commune (plus théorique qu'empirique) que, si deux chaînes apparaissent avec leur propre registre* de comptes, leurs UCN* et leurs règles protocolaires, seules les UCN* de la chaîne majoritaire seront considérées comme légitimes, conservant leur Tickers sur les bourses d'échange auxquelles est liée leur valeur de marché. À l'époque, les bourses d'échange affichent explicitement leur intention de suivre les décisions exprimées de la majorité. De plus, du fait d'un partage du même algorithme de consensus*, la chaîne minoritaire et ses utilisateurs (en particulier lesdites bourses) deviennent exposés aux attaques 51%, les opérateurs concurrents de la chaîne majoritaire disposant d'une puissance de calcul bien supérieure (cf. Annexe n°V.5). Dans ces conditions, la chaîne minoritaire doit rationnellement être désertée par les usagers, mais aussi par les mineurs restants. Leur profit en dépend : « *parce que cela n'a jamais été testé auparavant, [...] quand, des années avant même qu'Ethereum existe, les gens discutaient, que se passerait-il si vous Fork*iez le Bitcoin ? Tout le monde était d'avis que, au début, il y aurait deux chaînes, puis, à un moment donné, l'une d'entre elles mourrait [...] la grande majorité des gens s'attendaient à ce que l'une d'entre elles meure et que l'autre survive* » [Van de Sande, Entretien n°13]. Tous les acteurs confirment cette croyance, « *cela nous a pris... cela m'a pris par surprise [car les] gens qui prédisaient [...] que les deux chaînes allaient survivre [...] étaient une minorité importante.* » [Van de Sande, Entretien n°13]. À « *l'époque, je pensais [que la chaîne non Fork*ée allait] s'étioler et mourir [...] j'ai travaillé à la Fondation Ethereum à l'époque [...] une grande partie de mon état d'esprit, de mes croyances et tout le reste a été hérité de ça.* » [B. Summerwill, Entretien n° 26]. Pourtant, quelques heures plus tard, l'inimaginable se produit. La chaîne Fork*ée Ethereum va reprendre vie, sous l'impulsion d'une poignée de mineurs : avec le Fork*, « *quand les réseaux* se sont divisés... au début toute la puissance de hachage est allée dans la chaîne de Fork* et ensuite environ 10-20% du taux de hachage est revenu [...] il y a toujours une répartition 80/20* » [F. Vogelsteller, Entretien n°12, voir la répartition entre les deux en Annexe n°III.15.1]. Les membres de la cellule de crise observant le Fork* peinent d'abord à comprendre : « *Que se passe-t-il ? Quelqu'un perd de l'argent en minant une chaîne non rentable ? Pourquoi ?* » (A. Van de Sande Russo 2020, p. 207). Contre toute attente, une minorité de nœuds* du réseau* décide de continuer d'opérer l'ancienne chaîne non Fork*ée, qui devient « *un univers parallèle où l'Ethereum pré-Fork* rest[e] intact. Les comptes de chacun* » restent inchangés, ils disposent du même montant d'UCN* qu'avant le Fork* et les fonds de « The DAO » sont « *toujours bloqués dans la "Dark DAO"*, à une différence près et pas des moindres : les UCN* administrées au sein de cette chaîne ne sont pas des « *ether [mais] la cryptomonnaie* propre à cette chaîne parallèle* » (*Ibid.*, p. 206-207), l'*« Ether Classic »*. L'évolution de la puissance de calcul dédiée à Ethereum avant le Fork*

qui se maintient sur l'ancienne (voir Annexes n°III.5) est une mesure de l'intérêt des mineurs pour des UCN* qui n'ont encore aucune valeur marchande : ces mineurs « *ignor[ent] les incitations économiques immédiates* [et font le pari] que la cryptomonnaie* de la chaîne gagnerait plus tard en valeur et qu'ils seraient compensés ». Mais ce seul pari des mineurs ne peut expliquer à lui seul cette survie. Une CM n'est pas qu'un protocole que des machines font tourner. Leur attention étant absorbée par le *Fork**, peu d'*etheristes* se sont souciés de l'institutionnalisation du camp dissident.

Un *Hard Fork* contentieux inédit : la sécession d'Ethereum Classic

Le 10 juillet, en amont du *Fork**, un anonyme avait créé un répertoire Github appelé « *Ethereum Classic* » (ETHC). Dans un article de *Bitcoin Magazine*, Wirdum (2016) souligne que, si « *Ethereum Classic semble être une blague, destinée à faire valoir un point de vue, le projet a gagné une certaine traction, avec une base d'utilisateurs petite mais croissante sur Reddit et Slack, et avec la bourse décentralisée Bitsquare offrant son jeton - l'ether classique - comme une option d'échange* ». Sur cette plateforme d'échange, dans « *le carnet d'ordres [...] pour les transactions* Ethereum Classic/Bitcoin, [figurent] les trois premières offres à des prix allant de 6 800 ETHC/BTC (0,10 \$ par ETHC) à 10 000 ETHC/BTC (0,07 \$ par ETHC)* » (Shin 2022, p. 190). Le 21 juillet, Buterin reçoit un mail de Greg Maxwell, le *Core Dev Bitcoin Core* qui lui propose d'acheter ses ETHC, signalant son soutien à *Ethereum Classic*. Ce mail est interprété comme un camouflet : il « *enlevait son gant et giflait Vitalik au visage* » (Srir cité par Russo 2020, p. 207). Les réseaux* servent à populariser les ressources communautaires en construction : *sur BitcoinTalk, [l']utilisateur Seccour, [...] "bitcoiner, crypto-anarchiste et cypherpunk"* [publie] un fil de discussion intitulé "[ETHC] Ethereum Classic Speculation", [présentant] un nouveau logo [...] avec un logo similaire en double tétraèdre, mais en vert sur un fond noir [et comprend] des liens vers un explorateur de blocs Ethereum Classic, le Reddit Ethereum Classic, le Slack Ethereum Classic et le Wiki Ethereum Classic. » (Shin 2022, p. 190). Arivicco est le « coordinateur du projet ». Originaire de Russie, il conserve un strict pseudonymat parce que « *la situation juridique autour de la crypto est changeante et incertaine* » et qu'il est « *également le propriétaire de BitNovosti.com, le plus grand média crypto en langue russe, qui gère un site d'actualités, une chaîne YouTube, produit des films, etc.* » (*Ibid.*). Comme il l'explique, il n'est ni un « *troll* », ni « *l'attaquant* » : « *Il s'agit d'une initiative qui a vu le jour sur des forums en langue russe ; probablement parmi quelques douzaines de mineurs actifs, de traders et de développeurs* travaillant dans différents aspects de la crypto* », dont beaucoup se revendiquent « *partisans d'une position crypto-décentralisatrice radicale, [ils] pens[ent] que les systèmes de blockchain devraient toujours adhérer à trois caractéristiques : l'ouverture, la neutralité et l'immutabilité* [. Selon eux] le renflouement de la DAO sape deux des trois principales propositions de valeurs de la plateforme » (Arivicco cité par Wirdum 2016). Ces positions et les griefs envers Ethereum seront explicités dans une « *Déclaration d'Indépendance d'Ethereum Classic* », publiée le 15 août (Ethereum Classic et Arivicco 2016). Bien que reconnaissant de « *la création de la plateforme blockchain Ethereum par la Fondation Ethereum et ses développeurs* fondateurs* », cette « *communauté d'individus souverains [est] unie par la vision commune de continuer la blockchain Ethereum originale [...] sans censure, fraude ou tierce interférence* ». À partir d'une liste de ce qui a été perçu comme « *une longue série d'abus, en particulier par la direction de la Fondation Ethereum* » du fait de sa participation aux événements, cette déclaration affirme les valeurs cardinales que se fixe la communauté de paiement de cette CM sous la forme d'« *un code de principe* » : « *nous croyons en une blockchain décentralisée, résistante à la censure et sans permission. Nous croyons en la vision originale d'Ethereum en tant qu'ordinateur mondial qui ne peut pas être arrêté, exécutant des contrats intelligents irréversibles. Nous croyons en une forte séparation des préoccupations, où les Forks* de la base de code ne sont possibles que lors de la correction des vulnérabilités au niveau du protocole, des bogues ou de la*

mise à niveau des fonctionnalités. Nous croyons en l'intention initiale de construire et de maintenir une plateforme de développement résistante à la censure, sans confiance et immuable. [signé] La communauté Ethereum Classic » (Ethereum Classic et Arvicco 2016).

Bien qu'« Ethereum Classic » a « franchi la partie la plus difficile de la transition post-Fork* [en assurant] la survie de [la] chaîne », il reste beaucoup à faire du côté de son développement infrastructurel. Le 22 juillet, la communauté se dote d'un *ticker* conventionnel, l'« ETC », qui « contraste bien avec le ticker ETH qui est revendiqué par la chaîne Fork*ée, sans lui sembler de second ordre [car il] a "l'aspect et la convivialité" de pièces importantes telles que BTC, LTC... ETC » (Arvicco 2016b). C'est le 24, quatre jours après le *Hard Fork**, que l'importance structurelle des passerelles* d'échange va apparaître à tous. Pour certains, si « Ethereum Classic [...] a survécu [, c'est] uniquement parce que certaines parties se sont dit que c'était [...] des opportunités de trading supplémentaire et donc ont maintenu le truc complètement sous perfusion [:] si "Poloniex" [une bourse] n'avait pas fait ça, [...] le lister un week-end, je pense juste que personne n'aurait rien fait et le truc serait mort naturellement. » [N. Bacca, Entretien n°8]. En effet, la bourse Poloniex se dédie de ses engagements à ne suivre que la chaîne majoritaire et ouvre finalement le trading pour l'UCN* de la chaîne concurrente : par deux tweets, Poloniex annonce dans la journée l'ouverture des paires de trading « ETC/BTC et ETC/ETH » et que « tous les utilisateurs qui avaient un solde #Ethereum au moment du Fork* ont maintenant un solde correspondant de \$ETC » (Shin 2022, p. 194)⁴⁷⁹. Les bourses Kraken et Bitfinex suivent quelques jours plus tard, et Coinbase les rejoint la semaine suivante (Russo, p. 208), Avec les listings de l'UCN* ETC sur la plupart des grandes places de marché, le cours remonte brutalement (Annexe n°III.15.3), ce que célèbre la communauté en formation (Arvicco 2016a). Les incitations économiques s'affermisent et stimulent l'activité de minage : dès lors et pour quelque temps, il n'est pas rare que le rendement minier d'ETC soit supérieur à celui d'ETH, conduisant des mineurs à passer d'une CM à l'autre, sans tenir compte des sous-jacents philosophiques de chacune (cf. Annexes III.5.2). Le 25 juillet, Arvicco lance une campagne de recrutement, via un billet de blog intitulé « Que puis-je faire pour aider le projet Ethereum Classic ? » (Arvicco 2016c). Après les passerelles* d'échange, ce sont désormais des investisseurs/entrepreneurs qui s'intéressent au concurrent rigoriste d'Ethereum. Ce 25 juillet, Barry Silbert, l'« un des acteurs les plus influents de l'industrie du bitcoin, [et fondateur du] Digital Currency Group (DCG), qui investissait dans toutes sortes d'entreprises du secteur », annonce publiquement sur twitter un premier investissement dans les Altcoins* : « J'ai acheté ma première monnaie numérique non bitcoin... Ethereum Classic (ETC). À 0,50 \$, le rapport risque/rendement m'a semblé bon », avant d'annoncer que « Genesis Trading », qui lui appartient, facilitait les transactions* OTC d'ETC de gros (25 000\$ minimum, Shin 2022, p. 197). D'autres profils de poids, également « hostiles à Ethereum », viendront en soutien à Ethereum Classic : l'ex co-fondateur d'Ethereum devenu entrepreneur dans le secteur, « Charles Hoskinson, toujours mécontent [...] depuis son expulsion deux ans auparavant » tweete qu'il « n'aurai[t] jamais pensé tweeter cela... [il] réintègre Ethereum pour commencer à apporter des contributions à Classic » (*Ibid.*).

⁴⁷⁹Son CEO, « *Tristan [d'Agosta] était [intéressé] de voir comment Ethereum Classic fonctionnerait [et a donc] codé un smart contrat de split* » permettant de sécuriser la procédure de fork contre un risque particulier lié à ce type de fork : les attaques par rediffusion (ou « *replays-attacks* ») permettant à un attaquant d'intercepter des données de transactions valides diffusées publiquement sur l'une des chaînes, afin de les rediffuser modifiées dans l'autre afin de voler les fonds. Toutes les bourses listant l'ETC n'implémentent pas rapidement ce type de sécurité et « *il y a des gens qui ont perdu de l'argent sur d'autres exchanges puisque justement les autres exchanges n'avaient pas encore fait leur « split » correctement [...] il me semble que Coinbase a perdu de l'argent suite à ce problème* » [N. Bacca, Entretien n° 8].

Se séparer pour mieux se retrouver : fin d'une remise en ordre et ses enseignements

Du côté d'Ethereum, le retour à la vie d'*Ethereum Classic* pose de nouveaux ou plus exactement d'anciens problèmes au groupe du WHG : sur cette chaîne, « *the DAO Wars* » est toujours en cours, ils ne pourront empêcher l'attaquant de retirer ses ETC et, de leur côté, ils se retrouvent à devoir administrer des fonds liés au sauvetage libellés en ETC. C'est cette tournure prise par les événements qui conduit beaucoup des membres du « *Robin Wood Group* » à se désengager : le sauvetage des fonds sur Ethereum a été réalisé, ce qui se passe sur *Ethereum Classic* ne relève ni des mêmes considérations, ni des mêmes risques et incertitudes, particulièrement juridiques.

Le deuxième groupe, plus restreint, dit « *White Hat Group* », est alors constitué (cf. Tableau 10, Russo 2020, p. 207 ; Shin 2022, p. 202). « *Slock It* » s'était rapproché de Bity à des fins de conformité légale. Le WHG engage alors la même équipe pour « *protéger, sécuriser et plus tard distribuer les fonds équitablement sous une structure juridique suisse indépendante* » (Baylina, dans un post du 11 août, cité par Russo 2020, p. 209). Cette volonté de protection fait suite au fait que certains ont reçu « *des menaces juridiques, [...] et [Bity] a reçu des menaces [de] deux cabinets d'avocats [...] un en Suisse et un aux États-Unis [qui] étaient liés aux ETC.* » [A. Roussel, Entretien n° 11]. Restituer les fonds en Ether était assez simple et peu controversé. Mais le fait que lesdits fonds sont désormais dédoublés dans le monde parallèle d'*Ethereum Classic* pose des questions inédites, dont la première pour le WHG est de savoir s'ils restituent les fonds directement en ETC, sur la chaîne ETC, ou s'ils les convertissent en ETH et restituent sur le réseau* Ethereum. Avec le *Fork**, le WHG se retrouve à administrer « *7,2 millions d'ETC, soit environ 15 millions de dollars à l'époque, dans leur DAO enfant [afin de les] rendre à leurs propriétaires* » (Russo 2020, p. 207).

Cette période *post-Fork** présente « *un risque légal beaucoup plus élevé* » [A. Van de Sande, Entretien n°13]. L'option d'une restitution sous forme d'ETC apparaît la plus simple, « *mais après avoir discuté de la question avec Bity, ils ont décidé qu'ils devraient retourner les fonds en ETH [car, d'après] Griff, les investissements avaient été faits en ether, donc ils devraient être libellés en ETH* ». À cela s'ajoutait bien entendu une forte « *animosité générale envers Ethereum Classic* », dont la majorité pensait que l'UCN* allait perdre sa valeur rapidement et que ce n'était qu'une CM « *soutenue par les soi-disant maximalistes* Bitcoin qui voulaient voir Ethereum échouer ; ils ne voulaient pas contribuer à son succès en distribuant l'ETC aux investisseurs DAO* » (Russo p 209.). Vendre près de « *7,2 millions d'ETC sur le marché du jour au lendemain n'était pas facile* », le WHG et Bity arrivent à échanger seulement 14% des fonds en ETH et en BTC « *avant que les bourses de crypto-monnaie Poloniex et Kraken ne gèlent les comptes de Bity pour examiner les transactions** » (*Ibid.*, p. 209). Les fonds seront finalement libérés quelques jours plus tard afin d'être redistribués en ETC : au vu de la controverse et des difficultés suscitées, l'équipe échange ses ETH et BTC en sens inverse début septembre, l'opération réalisant même un profit. C'est le 13 août que Roussel (2016a) annonce le déploiement du « *Withdraw Contract* » sur *Ethereum Classic*, permettant de réclamer ses ETC contre ses DAO Tokens : « *ce contrat de retrait [,] déployé le 30 août [donnera à] tous les utilisateurs [...] 6 mois à partir de ce jour pour réclamer leur remboursement* » (*Ibid.*). Le 5 septembre, l'attaquant retire « *3,6 millions d'ETC, soit environ 5,5 millions de dollars à l'époque [...] du « dark DAO » sur la chaîne Ethereum Classic [et] une fois de plus fait un doigt d'honneur à Ethereum [réalisant un] don de 1 000 ETC au fonds de développement Ethereum Classic* » (Russo p. 2010). Le 6 septembre, les derniers fonds en possession du groupe sont versés au « *withdrawContract* » (Roussel 2016a). Le 30 janvier 2017, le délai d'activation du « *WithdrawContract* » servant à la résitution des ETC est étendu de deux mois, car si il « *a été largement utilisé par la communauté [avec] plus de 6 millions d'ETC [...] retirés, mais il y a encore des transactions* de retrait quotidiennes* » (Roussel 2017b). C'est finalement

le 15 avril 2017, avec la désactivation du « WithdrawalContract », que le travail de remise en ordre prend fin pour le WHG (Roussel 2017a).

La crise semble éteinte et les inquiétudes restantes attendront encore quelques mois avant d'être levées. Cette crise est hantée par les questions juridiques et réglementaires (ce qui illustre que les autorités de régulation participent indirectement du cadre de la décision des acteurs de la gouvernance *sur l'infrastructure*, d'où leur présence en légende de la Figure 13, pour Bitcoin) : c'est le cas lorsque l'équipe de « Slock It » se pose des questions liées à la levée de fonds, quant il s'agit de qualifier les DAO Tokens en des titres, mais aussi quand se pose la question du statut juridique de « The DAO », ou de la constitution de DAOLink comme véhicule permettant les interactions économiques. Enfin, les responsabilités dans la gestion de crise ont été interrogées et sont sources de menaces ; il en est de même pour ce qui est du WHG et de leurs différentes interventions. Tous les acteurs seront fixés le 25 juillet 2017, avec la publication d'un rapport d'enquête sur « The DAO » par la SEC (d'où le choix d'arrêter notre Chronologie 5 de cette remise en ordre à cette date) : enquêtant « *pour savoir si la DAO, une organisation non constituée en société, Slock.it UG ("Slock.it"), une société allemande, les cofondateurs de Slock.it et des intermédiaires pourraient avoir enfreint les lois fédérales sur les valeurs mobilières [,] la Commission a décidé de ne pas prendre de mesures d'exécution dans cette affaire sur la base de la conduite et des activités dont elle a connaissance* », alors même qu'elle reconnaît avoir « *déterminé que les jetons DAO sont des valeurs mobilières en vertu de la loi sur les valeurs mobilières de 1933 ("Securities Act") et de la loi sur l'échange de valeurs mobilières de 1934 ("Exchange Act")* » (Securities and Exchanges Commission 2017). Le rapport finit par rappeler un ensemble de réglementations afférentes et par inciter tous les acteurs qui « *utiliseraient une organisation autonome décentralisée ("Entité DAO"), ou d'autres moyens basés sur le ledger distribué ou la blockchain pour lever des capitaux, à prendre les mesures appropriées pour assurer la conformité avec les lois fédérales américaines sur les valeurs mobilières* » (*Ibid.*).

Cette crise du *Hard Fork** consécutif à l'attaque de « The DAO » est à la fois fondatrice pour *Ethereum* et *Ethereum Classic*, mais, plus généralement, pour l'écosystème crypto-monétaire. Derrière cette sécession protocolaire et communautaire inédite se cache d'abord la résolution d'un conflit idéologique traversant la communauté originelle d'*Ethereum* [V. Zamfir, Entretien n°9]. Dès la conception et durant cette phase de preuve de concept, il y a encore « *deux Ethereum [reposant sur] deux visions différentes [...] coexista[nt] au sein du même projet [:] certaines personnes étaient attirées par l'idée d'Ethereum en tant que Bitcoin programmable [, d'] autres voyaient Ethereum comme un "ordinateur mondial", une sorte d'Amazon décentralisé pour les applications (Dapps)* » [B. Summerwill, Entretien n° 26, mobilisant une présentation de Charles Hoskinson]. Cette crise va révéler que cette coexistence n'avait de pacifique que l'apparence. Ces sous-communautés ont finalement affirmé leur identité comme communautés de paiement séparées, « *ces deux visions bien que toutes deux intéressantes, étaient "mutuellement irréconciliables"* » [*Ibid.*]. Et c'est grâce au *Hard Fork** contentieux, et à la sécession monétaire qu'il permet, que ces communautés de paiement ont pu retrouver le semblant d'homogénéité en valeurs nécessaire, que la crise avait fait voler en éclat. Du côté d'*Ethereum* et malgré une culture *bitcoiners** qui leur faisait préférer la moindre intervention, la grande majorité se range du côté de la solution la plus radicale du *Hard Fork**, afin d'assurer la viabilité du jeune projet *Ethereum*. Les *Anti-Forks** considéraient que la réalisation d'un tel *Hard Fork** pour une faille d'application en ferait un précédent dangereux, entachant irrémédiablement la confiance dans *Ethereum*. Pourtant, et malgré les nombreux hacks et failles qui continueront de toucher à la couche applicative d'*Ethereum*, aucune autre intervention de ce type n'a été depuis réalisée : la communauté désapprouvera en effet par la suite ce type d'intervention [par exemple, dans le cas de bogues affectant l'implémentation multi-signature Parity et ses utilisateurs, J. de Tychet ; Entretien n° 4]. Finalement, Buterin (2017) et la communauté

Ethereum finiront par contester et nuancer ces *a priori* existants sur les *Forks** hérités des *bitcoiners** et feront du *Hard Fork** le sentier d'évolution privilégié d'Ethereum. Tout *Fork** qu'il soit, *Soft* ou *Hard*, il est coercitif à divers degrés. Mais quand on souhaite « *apporter un changement controversé* », les *Hard Forks*⁴⁸⁰ relèvent d'une coercition moindre, car ils offrent, comparativement aux *Soft Forks**, un plus grand éventail de choix, ce qui permet de « *mieux préserver la liberté des utilisateurs* ». Les *Hard Forks**, contrairement aux *Soft Forks**, sont « *opt in* ». En effet, l'ensemble des participants doit prendre part au processus de décision suivant qu'ils imposent une gouvernance publique et hybride : tout « *opérateur de nœuds** doit décider consciemment s'il doit installer un *hard Fork** pour que son *nœud** soit compatible avec les *nœuds** des opérateurs qui ont également décidé d'installer ce *hard Fork** » (Zamfir 2017). Les *Hard Forks** fournissent enfin un mécanisme de sécession sans lequel impossible de clamer son indépendance, comme le fait « *Ethereum Classic* » (The Ethereum Classic Community 2016), car l'ancienne chaîne peut continuer à exister, là où les *Soft Forks** « *favorisent institutionnellement la coercition par rapport à la sécession* », forçant les utilisateurs à accepter les nouvelles règles du protocole puisque la chaîne originale cesse d'exister. Ce cas a souligné à nouveau l'importance d'une diversité d'acteurs. Dans la réussite ou l'échec de cette sécession, si les mineurs et développeurs* Core sont nécessaires, d'autres acteurs tout aussi importants de la gouvernance *sur l'infrastructure* sont apparus, comme les bourses, qui jouissent de pouvoirs structurels importants (leur décision de listing donne vie aux incitations économiques de la chaîne sécessionniste). L'expérience *Ethereum Classic* apparaît sur une plus longue période comme un échec, la CM restant peu utilisée et n'ayant jamais vraiment concurrencé *Ethereum*. En fin de compte, la résolution de la crise de « *The DAO* » démontre que « *la partie importante de tout Fork*, Soft ou Hard Fork*, est que la grande majorité des nœuds* se mettent à jour* » [Corallo, Entretien n° 15] et que cette majorité d'acteurs non humains soit soutenue par l'ensemble des parties prenantes humaines qui en constitue la communauté d'usage.

Si cette crise a ouvert des précédents, c'est justement au niveau de sa gouvernance. À travers elle, la communauté Ethereum précise les voies permettant d'établir quelles modifications/corrections du protocole étaient pour elle désirables et légitimes. De bonnes pratiques et des procédures d'expression des désaccords et d'élaboration de consensus *ad hoc* ont été institutionnalisées : la procédure des EIP, inspirée des BIP Bitcoin, allait être complétée de différents mécanismes permettant de coordonner une diversité d'équipes d'implémentation client différentes, inclure des arènes de discussion vidéo avec transcription accessible à la communauté (les *All Core Dev Meeting*, J. de Tychet, Entretien n° 4 ; B. Summerwill, Entretien n° 26]. Les problématiques posées par la mesure du soutien communautaire aux *Forks** ont montré que : « *la gouvernance sur Ethereum, elle fonctionne vraiment avec des signaux. C'est vraiment [...] ce qui s'est passé autour de la DAO, ça a été un bon, un bon stress test, on va dire et en fait, tout ce qui s'est passé après, ça a été tiré des leçons de ce qui s'est passé au moment de la DAO pour essayer de clarifier les signaux et d'être moins dans... des signaux qui sont moins facilement manipulables* ». » [S.Polrot, Entretien n°16]

⁴⁸⁰ Au sein des *Hard Forks*, Buterin (2017) distingue : les « *Stricky expending Hard Forks* » qu'il préfère en ce qu'ils correspondent à une extension stricte de l'ensemble des transactions valides au sein des anciennes règles canoniques offrant une rétrocompatibilité et les « *Bilateral Hard Forks* », qui induisent, eux, que les deux ensembles de règles protocolaires sont mutuellement incompatibles.

III.4 CONCLUSION DU CHAPITRE III

Ce troisième chapitre portait sur la gouvernance – *par et sur* l’infrastructure – des CM à l’aune d’une enquête sur la fabrique et la gouvernance de leurs crises. Le caractère polycentrique de leur gouvernance identifié comme singularité monétaire (cf. hypothèse conclusive du chap. II) y a été étudié au travers de la documentation et de l’analyse de deux cas de crises situées : la crise Bitcoin CVE 2018 et la crise du *Hard Fork** d’Ethereum consécutive à l’attaque de « The DAO ». Cette focale des crises de CM nous a permis de réfuter très directement l’ensemble des prétentions libérales-technicistes véhiculées qui font des CM des monnaies acéphales et décentralisées, autonomes et parfaitement apolitiques du fait qu’elles seraient régulées uniquement par le code et non par des entités gouvernantes. Cette même focale a permis de montrer que la confiance qu’accordent les *coiners** à leur CM, loin d’apparaître fondée exclusivement sur leur autorité algorithmique, repose bien plus sur des autorités communautaires et l’institutionnalisation de capacités communes d’intervention permettant de remédier à une situation au cas où le code et ses régulations déraillent. Ce travail nous a aussi offert un point de vue privilégié sur l’hétérogénéité des représentations traversant les communautés de *coiners**, sur ce qui fait des CM de « bonnes » ou « mauvaises » monnaies. En effet, à travers la normalité qu’ont dessiné nos états de crise, ce sont les propriétés désirées des CM qui étaient éprouvées et renégociées. Finalement, ce chapitre a permis de préciser dans quelle mesure cette gouvernance polycentrique pouvait soutenir effectivement la « *formation de consensus entre des individus mis par des intérêts politiques et commerciaux* » différents (De Filippi et Loveluck 2016, p. 15) en offrant à l’ensemble des *coiners** la capacité de participer à l’érection des décisions les concernant. La résolution de la crise d’Ethereum, qui a conduit à la sécession d’Ethereum Classic, a permis notamment de mettre en perspective l’idée que la gouvernance des CM, par la pratique toujours possible du *Fork**, garantit qu’aucun groupe ou entité issu(e) d’une des composantes communautaires n’apporte discrétionnairement « *au code une modification que la communauté désapprouve [car] celle-ci pourrait tout simplement refuser d’exécuter le nouveau code [à la manière d’un] “pouvoir de veto” [assurant] que la légitimité du code repose en fin de compte sur les utilisateurs* » (*Ibid.* p. 14).

Le premier temps de la démonstration a été consacré à la présentation périodisée de la crise Bitcoin CVE 2018, ouverte suite à la réception par des membres de l’équipe Bitcoin Core d’un rapport de divulgation responsable les informant de l’identification d’un bogue dans les codes logiciels permettant de contourner les régulations contre la double dépense*, donc de son monnayage. La restitution des événements, de la mise en crise à la remise en ordre, a permis de retracer les modifications du protocole Bitcoin, en explicitant leurs contextes, les acteurs à l’œuvre et les justifications qui président à leur développement, les procédures collectives de contrôle des modifications et les canaux de communication spécifiques mobilisés. Nous avons encore explicité les acteurs et les dispositifs socio-techniques clefs de la maintenance des codes protocolaires d’une CM, et interrogé les conditions de la découverte du bogue, de son évaluation, de sa correction et de sa publicisation, sous la forme d’abord d’un correctif mis à disposition de la communauté sans que soit révélée l’étendue des changements qu’il contient. Les informations critiques ont finalement été rendues publiques tardivement, à la faveur d’un processus de publication graduel. Pour mieux saisir le cadre et les enjeux de cette crise, nous l’avons ensuite resituée dans une histoire plus large des crises traversées par Bitcoin et sa communauté (cf. Chronologie 4) : bogue d’inflation, de scission de chaîne, DOS, PR, BIP, merge, *Soft Fork** ou *Hard Fork**, etc.

Le second temps du chapitre a été consacré à l’analyse de la politique de la crise et à l’identification d’une structure générale de gouvernance de Bitcoin, avec un code largement dominé par l’implémentation et les versions Bitcoin Core, une situation qui conduit à donner un poids important à son équipe de développement – les Core Devs – et au répertoire d’administration de ses

codes – le repo Bitcoin Core Github. Si l’analyse de l’administration des codes Bitcoin Core a démontré l’existence d’une hiérarchie formelle entre les « Core Devs », dotant certains acteurs de priviléges étendus, voire léonins (pour le mainteneur principal), il est apparu que la communauté Bitcoin s’était dotée de garde-fous permettant d’encadrer strictement l’ensemble des activités de développement. Des dispositifs et procédures variés sont mis en œuvre afin d’assurer la traçabilité des modifications proposées et implémentées (le *système d’intégration continu basé sur des vérifications de clefs PGP de confiance*), comme l’intégrité des nouveaux codes sources Bitcoin Core publiés (*Gitian Building*) . Ces dispositifs visent à préserver la possibilité pour les participants d’accepter ou de refuser librement, et de manière éclairée, toute nouvelle version publiée (existence de dispositifs de mesure du consentement et de fixation de la majorité *via* des dispositifs de vote, de signalement et d’activation). La crise Bitcoin CVE 2018 et la gouvernance qu’elle nous a permis d’analyser, bien que d’apparence hautement centralisée et technocratique et à l’opposé de l’idée de gouvernance polycentrique où « *tout le monde [est] d’accord avec la direction que prennent les choses* » [M. Corallo, Entretien n°15], ne représentait en fait que l’une des deux faces de la gouvernance de crise des CM : sa face routinière, que nous qualifions de *huis clos*. Sa caractéristique est justement d’être réservée à des crises dont la remise en ordre induit *a priori* un consensus fait d’absence de dissensus. Dans le cadre de cette gouvernance de *huis clos*, les « Core Devs » bénéficient de discrétion dans la production d’un consensus d’abord local au sein d’un groupe de quelques techniciens amis. Ce cas présente un type particulier et renvoie à une crise que nous qualifions de *crise de vulnérabilité*, car relevant d’une situation où les résultats des codes sont en contradiction flagrante avec les attendus communautaires. Ce type de crise s’oppose aux *crises d’évolution*, qui concernent des situations où le code, bien qu’il fasse jusque-là ce que l’on attend de lui, est mis en crise par l’expression d’une volonté communautaire de le faire évoluer. La remédiation de la crise de vulnérabilité était simple et consensuelle, ce qui explique l’absence de dissensus observé localement d’abord, puis globalement après la divulgation complète de l’équipe Core. Cette gouvernance de *huis clos* met au jour une reconnaissance routinière, tacite et sans ambages de l’autorité des « Core Devs ». Mais celle-ci reste néanmoins suspendue au maintien du consensus autour des codes ainsi publiés. Qu’un acteur en conteste le bien-fondé et arrive à faire apparaître un dissensus les concernant dans la communauté, et la crise verra sa gouvernance se transformer en sa face opposée : la gouvernance « *publique* », spécifiquement taillée pour produire un consensus large concernant des modifications de codes *a priori* controversées.

Le troisième temps du chapitre fut dédié au cas de la crise du *Hard Fork** consécutif à l’attaque de « The DAO ». Ce cas illustre une crise *d’évolution* à gouvernance *publique* conflictuelle. Le protocole Ethereum fonctionnait comme attendu, mais il a été mis en crise par la proposition de l’utiliser comme moyen de remédiation afin d’annuler l’attaque et de restituer les fonds aux investisseurs. Ce type de crise, exceptionnel, conduit inéluctablement à des controverses, dont il est attendu qu’elles soient résolues en public et à grand bruit. Dans de tels cas, les stratégies de remédiation sont multiples - sont possibles : *Soft Fork**, *Hard Fork**, contre-attaque, ne rien faire - selon l’évaluation et les cadrages retenus des enjeux de la crise. Au centre de ces choix réside la question de leur légitimité reflétant l’hétérogénéité des vues communautaires sur les propriétés désirées de leur CM (immutabilité *versus* sauvegarde de la communauté) et de la « bonne » gouvernance qui y est associée (non-intervention par principe *versus* adaptation à une situation donnée). Finalement, dans une situation complexe et contrainte par l’urgence, la gouvernance de cette crise *publique* d’Ethereum lui aura permis de produire un consensus majoritaire relativement massif, incluant ses parties prenantes non humaines (nœuds* mineurs et complets), mais aussi humaines (utilisateurs finaux, services marchands et passerelles*, mineurs, etc.) *via* l’élaboration distribuée de mécanismes d’expression d’accords ou de désaccords variés et adressés aux différentes composantes communautaires. Ainsi, la minorité d’*etheristes* qui refusait cette solution du haut de leur interprétation rigoriste du slogan « *Code is Law* » ne se l’est pas vu imposée de manière

coercitive. Là où une modification de type *Soft Fork**, traditionnellement privilégiée sur Bitcoin, n'aurait pas permis à une nouvelle chaîne d'émerger, celle de type *Hard Fork** a bien permis de faire souverainement sécession et ce, hors coercition.

Ce chapitre a démontré que les CM ne pouvaient se prévaloir de s'être détachées de toute gouvernance humaine, comme l'affirment certains de leurs promoteurs. Ce n'est pas une mauvaise nouvelle car, en leur absence, Bitcoin, Ethereum ou toute autre CM n'aurait pas dépassé le stade de la preuve de concept et aurait été incapable de traverser leurs premières crises *de vulnérabilité* et d'arriver à s'optimiser, ou à évoluer radicalement pour s'adapter à un environnement changeant – *via des crises d'évolution*. N'en déplaise aux *coiners** du camp de la *règle radicalisée*, quand la lettre du code n'en respecte pas l'esprit, il reste - en dernier ressort – la primauté du consensus social sur les règles protocolaires. Une primauté dont toutes les crises, qu'elles soient *de vulnérabilité* ou *d'évolution* attestent, indépendamment de la forme prise de la gouvernance (de *huis clos* ou *publique*).

Ce chapitre a aussi permis d'ordonner et d'analyser en partie la complexité et la diversité des mécanismes de gouvernance des CM, Bitcoin et Ethereum. Néanmoins, les éclairages apportés par ce travail découvrent des zones d'ombres et des angles morts. Notre focalisation sur les crises protocolaires a conduit à s'intéresser principalement à la gouvernance *sur* l'infrastructure de Bitcoin et Ethereum, leur protocole, alors que des crises infrastructurelles, comme dans les cas de Mt Gox et Silk Road (Musiani, Mallard et Méadel 2018; cf. chap. I), peuvent impacter leur communauté et questionner leur monétisation. De par les choix de crise que nous avons faits, notre analyse octroie une place centrale à l'étude de l'administration du répertoire Github des implémentations protocolaires par le groupe des « Core Devs ». Cette place donnée à l'un des systèmes de ressources (essentiel il est vrai) participant du système de ressources plus large que représente l'infrastructure d'une CM laisse aux marges les autres composantes (et les systèmes de ressources qu'elles constituent) de ces communautés, ce qui mériterait d'être interrogé et réarticulé par des recherches spécifiques (sur les mineurs, les services marchands et les passerelles* en particulier, plus difficiles d'accès). Des questions importantes ont donc été soulevées sans toutes trouver de réponses suffisamment étayées, comme la question du financement des développeurs*, donc à la fois du renouvellement des compétences communautaires nécessaire à la gouvernance des CM . Ou encore, la question de la dépendance économique induite par les voies de financement actuelles qui posent des questions de conflit d'intérêts. Le poids relatifs de certains acteurs clefs, comme les bourses d'échange dont le rôle dans l'apparition d'Ethereum Classic a été souligné, mériteraient aussi d'être mieux compris. Toutes ces questions sont donc renvoyées à des recherches ultérieures.