Maël ROLLAND

Doctorant au CEMS | PhD candidat @EHESS

Lecturer in economics & crypto-currencies (@EHESS ; @ESILV; @ESGI, @ESC-Clermont & Strate)

@elmalandr0

rolland.mael@hotmail.fr

"Hercule et l'Hydre de Lerne" Pier Jacopo Alari Bonacolsi (Antico) - bronze - 32 x 32 cm - 1490 - (Museo Nazionale del Bargello (Florence, Italy) →

" Hercule combattant l'hydre de Lerne, figure de l'hérésie - Gallica.bnf.fr ←

"De la gouvernance des crypto-monnaies : pour un cadre d'analyse multidimensionnel"

Maël Rolland

Enseignant dans le supérieur -
Doctorant au CEMS-EHESS

FINTECH RISK MANAGEMENT
www.fintech-ho2020.eu

Introduction :

Bitcoin et l'émergence du phénomène crypto-monnaie

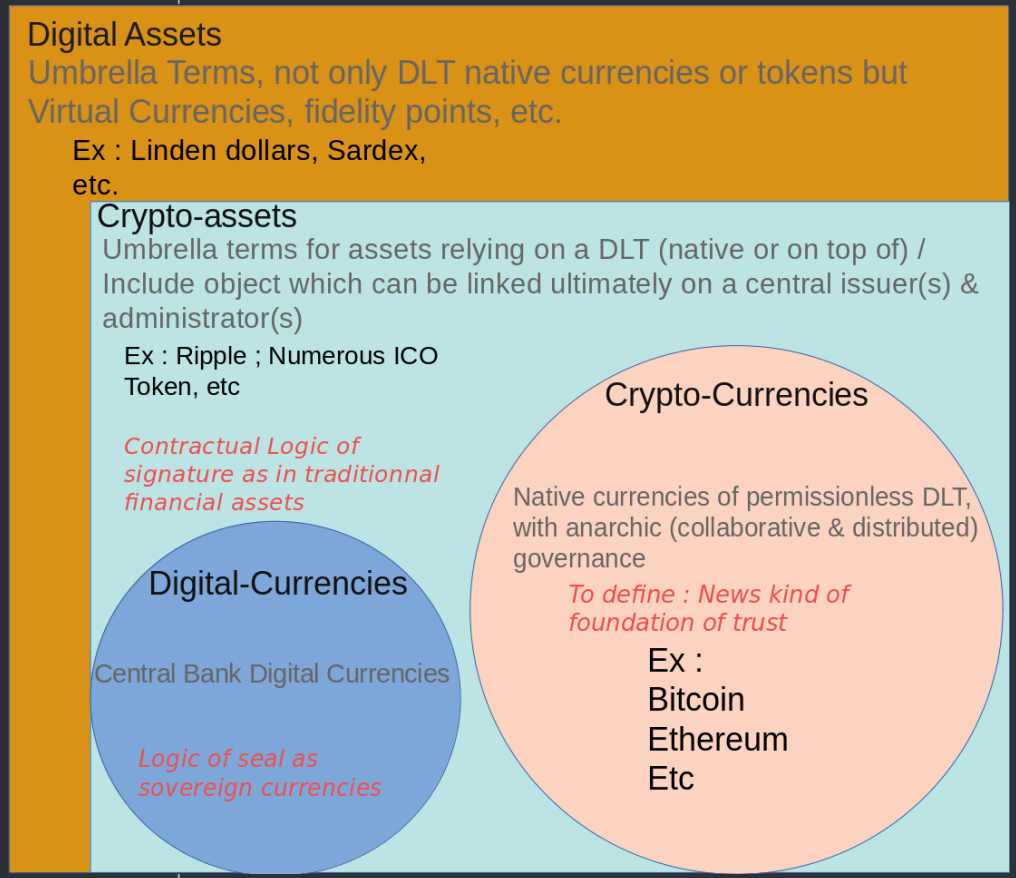
Bitcoin et son bitcoin

- lancement : 2009
- aujourd'hui :
  - une "capitalisation de marché" de près de 692 milliards de $,
  - un volume d'échange quotidien, sur les bourses d'échange, de 65 milliards (coingecko.com, 07/01/2021)
  - Quotidiennement, environ 300 000 transactions, émanant de près d'1 millions d'adresses actives uniques, pour une valeur médiane d'environs 800 000$ (bitinfocharts.com, 07/01/2021)

Les altcoins

- Près de 6130 CM ou apparentées
- 419 places d'échanges
- Capitalisation totale de plus de près de 1 021 602 460 678 $ (67 % pour BTC et 13,3 pour Ethereum ; coingecko.com, 07/01/2021)

Objet de notre recherche



Distinguer crypto-monnaies, monnaies digitales et crypto-actifs

Intérêt de l'usage du terme **crypto-monnaie** :

(i) affirmer leur essence proprement monétaire (ce qui fait débat).

(ii) souligner leur caractère inédit dans le champ monétaire :

- **consensus multi-partie**
- **gouvernance communautaire, distribuée et polycentrique**
- absence **de pouvoir discrétionnaire sur l'infrastructure** et sur **les données endogènes** consignées.

Bitcoin et l'émergence du phénomène crypto-monnaie

Ambitions des CM en terme de gouvernance :

➢ offrir des systèmes monétaires et de paiements **décentralisés, viables, efficaces, transparents, ouverts à tous et non censurable**.

Revendications :

- ❖ être des systèmes de paiement **"sans confiance"**
  - ➢ [illegible] nœuds dont **la structure et les** [illegible]

La monnaie serait garantie par un **consensus "mathématique" et non "politique"**

- ❖ substituer la gouvernance monétaire actuelle par un **ensemble de règles protocolaires intangibles**.

- ❖ offrir des "monnaies saines"
  - ➢ monnayages (quantités de monnaie émise, taux et règles d'usage) **fixes, transparents et crédibles**

I. D'un concept de gouvernance problématique à la problématique de la gouvernance des CM

D'un concept de gouvernance problématique…

- ➢ un concept controversé car polysémique
- ➢ absence de définition unique, rigoureuse et stabilisée

Deux grands types d'usages :

1/ Usages normatifs et politiques :
redéfinition du périmètre, des objectifs et des moyens de l'action publique

- ➢ La **"bonne gouvernance" se traduit par un "État minimal"**
- ➢ **Penser des politiques (policy) en dehors du politique (politics)**

2/ Usages positifs et scientifiques :
mobilisé dans l'analyse de **cas empiriques situés**

- ➢ Questionner les processus à l'oeuvre dans l'élaboration de compromis collectifs et la légitimité des consensus atteints.
- ➢ Permet d'interroger la multiplicité :
  - **des acteurs** (privés et publics)
  - **des formes** et **des modalités de résolution de conflits** et à **l'obtention de consensus.**

D'un concept de gouvernance problématique…

Le débat du pouvoir monétaire des gouvernements : "Rules *versus* Discretion"

Oppositions sur la nature de la monnaie et sur sa "bonne gestion" par les autorités monétaires :

- Pour **les tenants de la neutralité monétaire**,
  la "bonne gestion" de la monnaie par les banques et les banques centrales (BC) :
  - assurer seulement **la stabilité de l'unité de compte**
  - mise en place de **règles et de contraintes fortes** pesant sur la politique monétaire et les autorités qui en ont la charge

- Pour les autres,
  - **la stabilité du système de paiement** peut **primer** sur la stabilité de l'unité de compte
  - bonne gouvernance = capacité des autorités monétaires de réaliser des **actions discrétionnaires** afin d'éviter tout effondrement systémique

D'un concept de gouvernance problématique…

Les CM réactivent ce débat récurrent en économie monétaire de manière radicale.

➢ un concept de gouvernance en partie rejeté au sein de leur communauté :

- mobilisation du concept pour en critiquer les formes existantes
- un rejet hérité de la pensée cypherpunk et crypto-anarchiste

Des représentations à l'œuvre hétérogènes

➢ 2 idéaux-types :

(i) Affirmation de l'absence de gouvernance

(ii) Reconnaissance d'une gouvernance et volonté de la minimiser

D'un concept de gouvernance problématique…

(i) **Affirmation d'une absence de gouvernance** :

- consensus = résultat d'un pur processus technique "objectif" et des incitations qu'il fonde, en dehors de toute intervention humaine, débats et choix politiques, toujours conçus comme "subjectifs" et sous-optimaux.
- Processus objectifs définis et régulés par des règles protocolaires "immutables"

D'un concept de gouvernance problématique…

(ii) **Reconnaissance - plus ou moins tacite - de l'existence d'un gouvernance et volonté de la minimiser** :

- absence revendiquée de gouvernance
- MAIS **des processus de décisions des acteurs et des arrangements multiples** qui permettent l'évolution du protocole.
- des changements conditionnés à la **rétrocompatibilité** des différentes implémentations logicielles.
- soumission à **un consensus communautaire à quorum élevé**

"Je pense qu'une partie importante de ***ce qui fait Bitcoin Bitcoin, est de savoir quel est le processus d'évolution****, non ?"* (Matt Corallo, Bitcoin Core Dev; Entretien n°15)

➢ **Aussi, quand bien même elle serait ascendante, anarchique, implicite, informelle et minimale, c'est bien une "certaine forme" de gouvernance qui se dessine.**

… à la problématique de la gouvernance des CM.

➢ Une littérature académique centré principalement sur l'infrastructure technique

➢ Ambivalence des travaux portant sur la question de leurs gouvernances :

- en creux, existence de dimensions sociales articulant la "matérialité pratique" de Bitcoin aux dimensions matérielles, axiologiques et sémiotiques de la communauté (Maurer, Nelms et Swartz 2013 ; Desmedt et Lakomski-Laguerre 2015)

- MAIS focale sur la gouvernance *par* l'infrastructure :
  - architecture technologique
  - relations au **sein de la chaîne**

= modalité unique de gouvernance

⇒ **Angle mort**, voire négation explicite (Dupré, Ponsot et Servet 2015) des nombreuses relations sociales - et leurs arrangements - qui ont lieu **hors chaîne**.

⇒ Certain travaux font exception et s'intéressent à la dimension hautement communautaire de Bitcoin et des CM (Dodd 2017; Orléan 2019) comme à leur gouvernance duale (De Filippi et Loveluck 2016, Rolland et Slim, 2017; Hsieh, Vergne et Wang 2018; Musiani, Mallard et Méadel 2018).

… à la problématique de la gouvernance des CM.

Des mécanismes de coordinations différents :

(i) La gouvernance "*avec" ("governance with)"*

(ii) La gouvernance *"par" ("governance by")*

(iii) La gouvernance *"sur"* ("governance of")

La gouvernance des CM dévoilée par leurs crises.

Les phénomènes de crise : fonctions heuristique et herméneutique primordiales

- les crises, un moment privilégié d'étude où la monnaie se « dévoile » (Théret, 2007).
- Interruption du « fonctionnement routinier de la monnaie »

Au sein du champ des CM, différents types de crise peuvent apparaître, découvrant les diverses dimensions de leur gouvernance :

- Des conflits/débats communautaires concernant les évolutions du protocole
- Des bogues, des failles, des attaques aux niveaux des codes protocolaires
- Des hacks et des exploitations de failles non directement liés au protocole :
  - piratage de bourses d'échanges
  - défaillance de *Smart Contract* et perte des avoirs
  - compromission de portefeuilles individuels…

II. La gouvernance multidimensionnelle de Bitcoin

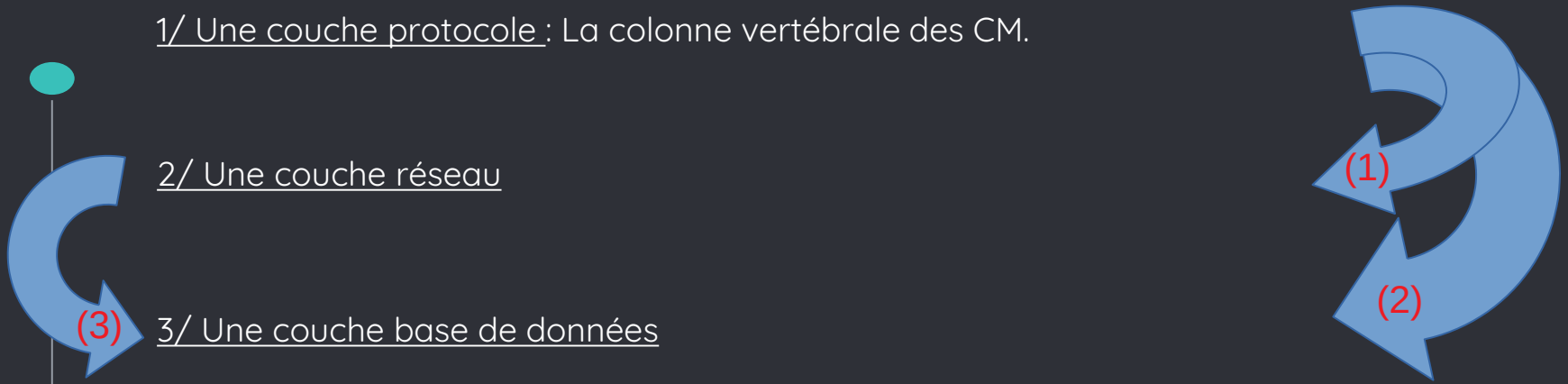
De la gouvernance *par* l'infrastructure : le protocole, ses processus et ses acteurs

L'infrastructure protocolaire des CM repose sur 3 couches clés interdépendantes et qui tissent entre elles des relations hiérarchiques (↻) ⇒ les caractéristiques du protocole pourraient être modifiées (réorganisation/censure du TX, …) et pourraient réintroduire la ***confiance*** intuitu ***personae.***

1/ Une couche protocole : La colonne vertébrale des CM.

2/ Une couche réseau

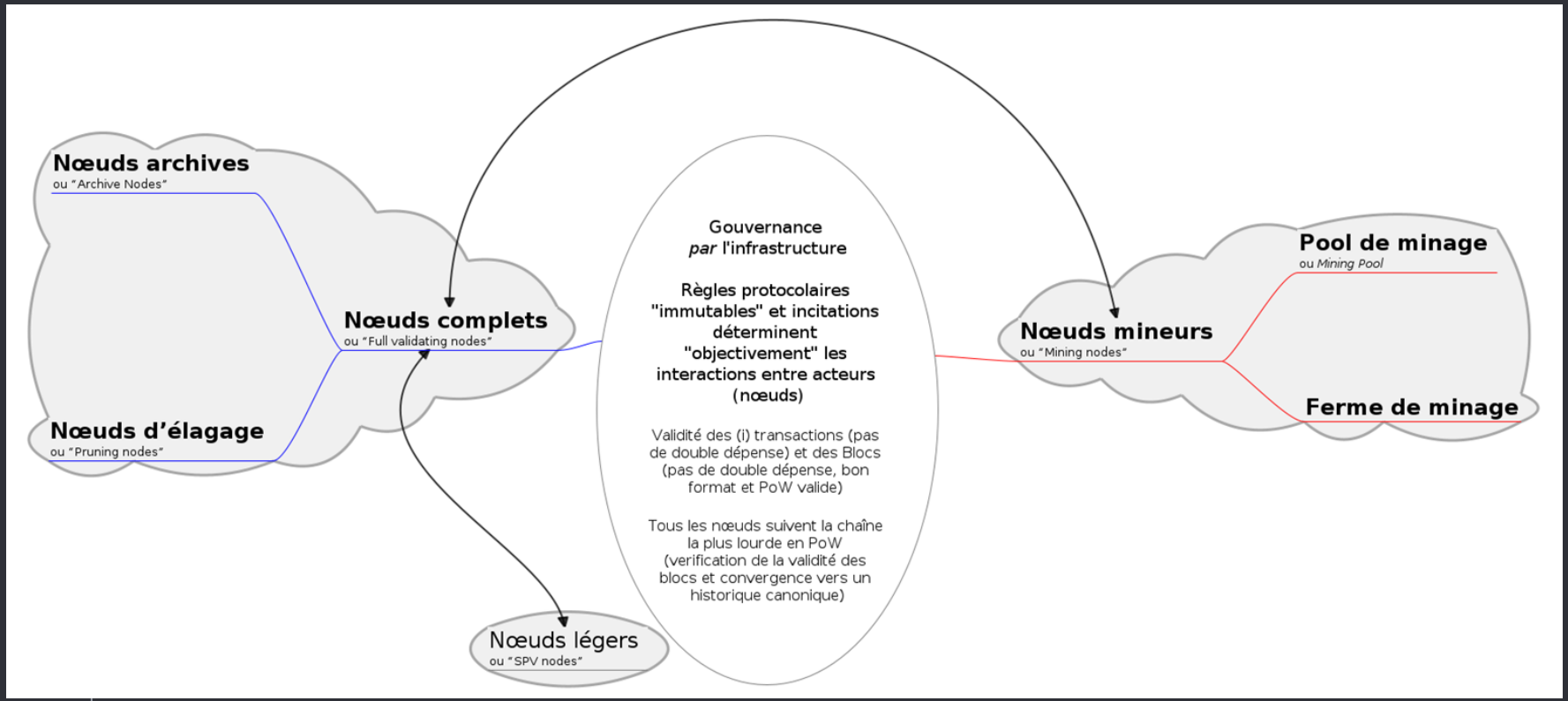
3/ Une couche base de données



⇒ Chaque ***couche*** est composée **d'un *ou de plusieurs éléments*,** qui correspondent à un ensemble de processus activés par les ***acteurs*** pour atteindre un ***ou plusieurs objectifs*** spécifiques.

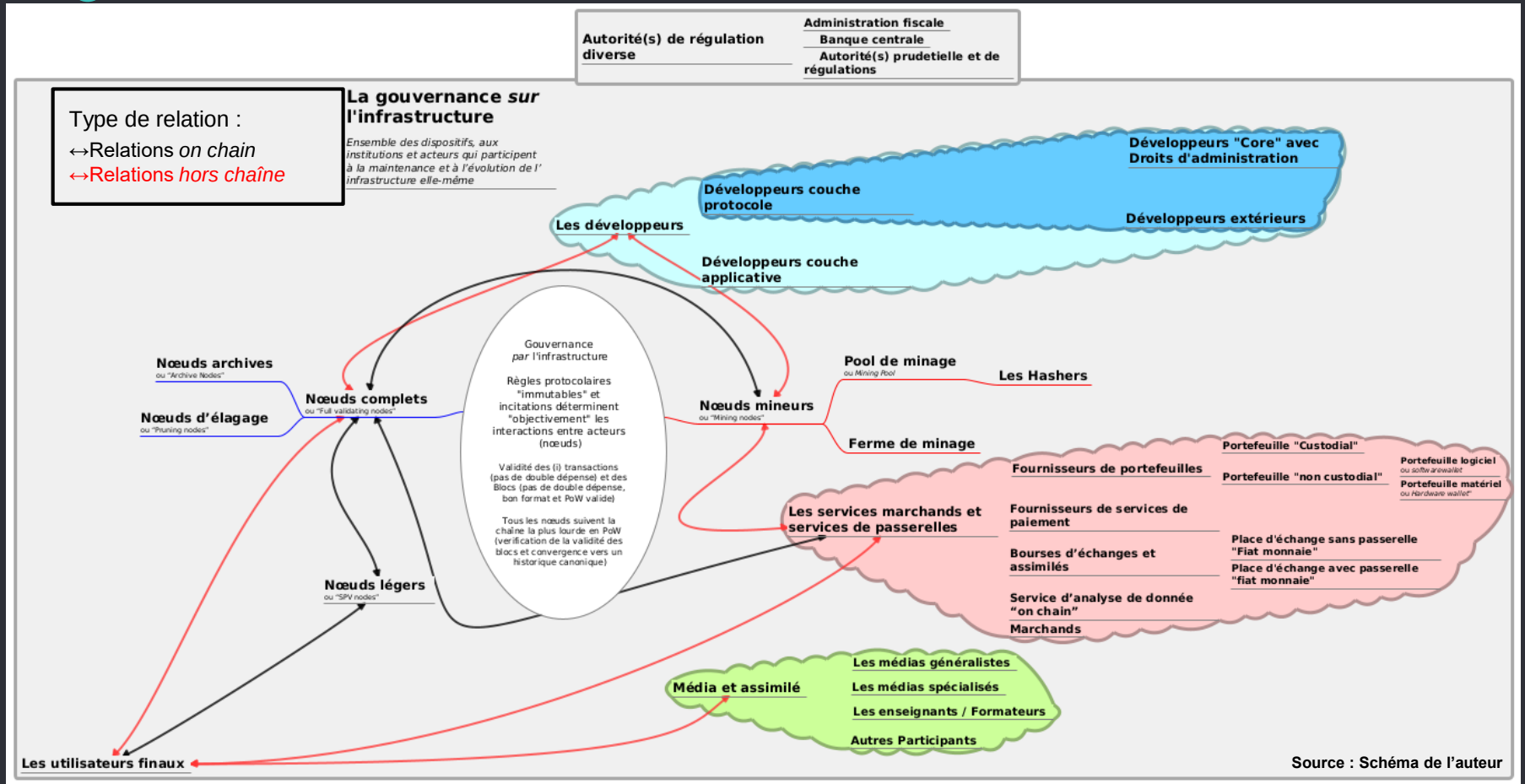
De la gouvernance *par* l'infrastructure : le protocole, ses processus et acteurs

Les acteurs définis formellement au sein du protocole et leur interaction



… à la gouvernance *sur* l'infrastructure.

Les partie-prenantes hors protocoles : autant d'acteurs de la gouvernance *sur* l'infrastructure

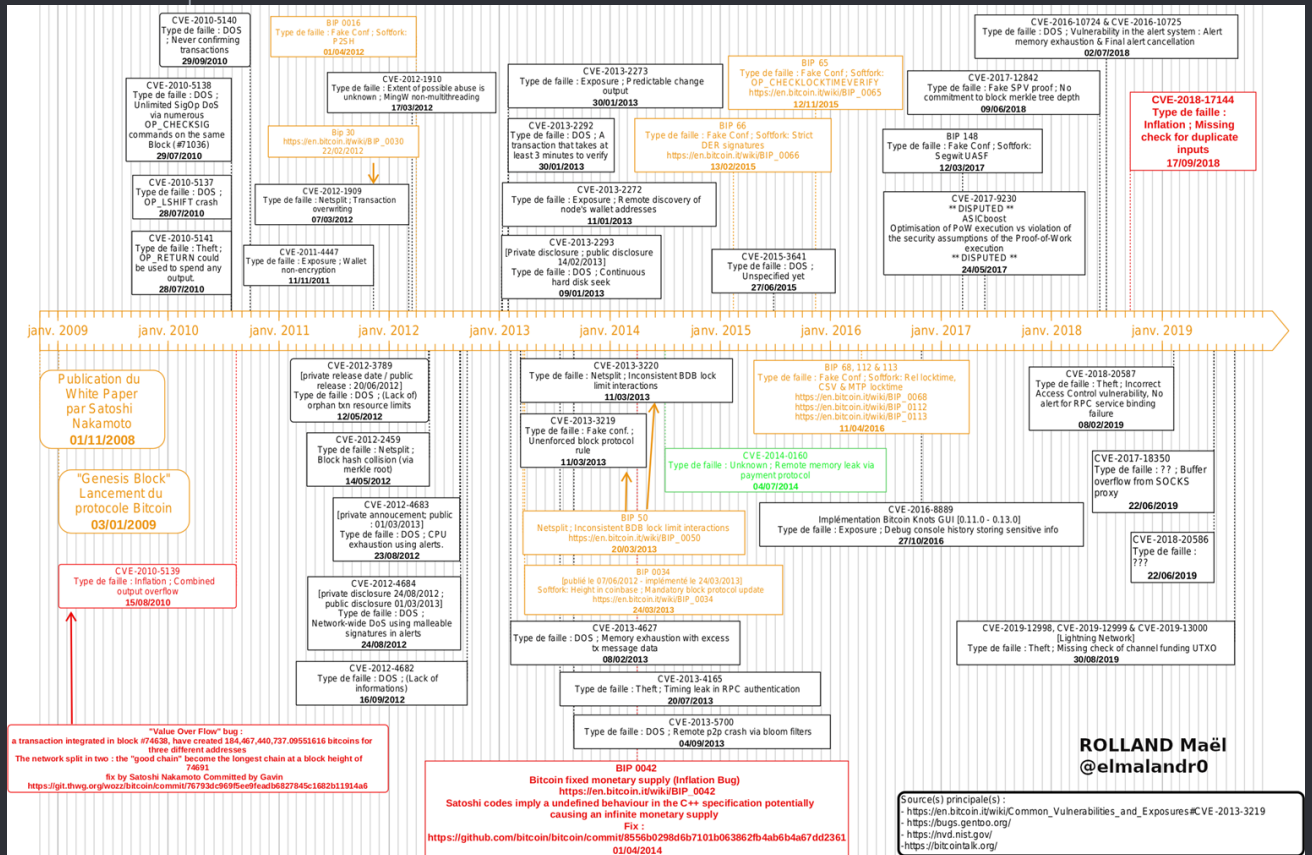


Source : Schéma de l'auteur

III. La gouvernance multidimensionnelle de Bitcoin dévoilée par ses crises

Bitcoin et ses crises liées aux modifications des codes protocolaires.

La **gouvernance *par* l'infrastructure** du Bitcoin suppose une **gouvernance *sur* l'infrastructure, extérieure et sociale**.



- Question de sa structure et de sa capacité à apporter des réponses à des **problématiques relevant de coordinations non uniquement techniques**.
- Différents types de changements techniques, qui n'entraînent pas les mêmes conséquences pour les membres de la communauté : Soft Fork vs Hard Fork
- L'histoire de Bitcoin est liée à ses crises passées et à leurs résolutions

La controverse de "la montée en charge" ("scaling debate") sur Bitcoin et sa résolution

Problématique récurrente concernant la capacité de Bitcoin à traiter une quantité de transactions croissante

Question des moyens disponibles pour faire augmenter la capacité de traitement de Bitcoin ⇒ **touche la totalité des membres de la communauté**.

Acteurs clefs :

- Les développeurs (propositions et analyse des solutions)
- Les bourses d'échanges (listing de future, "price discovery)
- Les Mineurs (signalement de préférence, choix d'accepter ou non la nouvelle implémentation logicielle)
- Les nœuds complets (signalement de préférence, choix d'accepter ou non la nouvelle implémentation logicielle)
- Les services marchands (annonces de soutien à des propositions)
- Les médias et assimilés (participation au débats, explications des arbitrages, etc.
- Les utilisateurs finaux (signalement de préférence en choisissant les services marchands qu'ils utilisent)

Diverses solutions proposées :

SEGWIT

(i) optimisation des transactions au sein d'un bloc inchangé

(ii) augmentation de la taille du bloc afin qu'il contienne davantage de transactions - entraîne des coûts et des avantages différents.

⇒ Renvoie aux représentations que les acteurs se font de Bitcoin et de ce qu'ils entendent par "argent sain". Besoin de construire un large consensus autour de ses propositions et représentations

Le Bogue Bitcoin Core CVE 2018 #17144 : quand une optimisation cache une remise en cause des règles consensuelles canoniques.

Le problème :

Découverte le 17 septembre 2018 d'une faille : Bitcoin Core CVE-2018-#17144

➢ elle ne touche que certaines implémentations et versions des clients logiciels des implémentation Bitcoin Core et Bitcoin Knot = ne concerne qu'une partie des nœuds.

Cette faille n'a pas les mêmes conséquences suivant la version logicielle et induit un double risque :

(i) Risque d'attaques par déni de Service (DOS) permettant de faire cracher les nœuds du réseau et donc de perturber son bon fonctionnement

(ii) Risque d'attaque par double dépense (plus grave)
= un bloc de transaction contenant une transaction dépensant plusieurs fois la même UTXO, sera considéré comme valide par les nœuds des versions 0.15.x.

⇒ « la faille la plus catastrophique que Bitcoin ait connue » (Awemany, 2018)

Cette itération de la faille nous **ferait sortir des règles de consensus reconnues de tous**, à la fois au niveau **de la validité de transactions** et **des blocs** et vis-à-vis du monnayage de Bitcoin (**règles d'émissions reconnues de tous** et **règles de circulation**).

Le Bogue Bitcoin Core CVE 2018 #17144 : quand une optimisation cache une remise en cause des règles consensuelles canoniques.

Les acteurs et processus impliqués dans cet événement :

Dans un premier temps :

- Les développeurs (découverte des failles, analyse des solutions, prise de contact avec une pool de minage)
- Les Mineurs (ici Slush Pool, reception du patch, analyse de celui-ci et mise à jours de la pool de minage pour sécuriser le réseau avant annonce publique de l'étendue de la faille)

Dans un deuxième temps :

- Les nœuds complets (si concernés par la faille, mise à jours rapide de son implémentation logicielle)
- Les services marchands (si concernés par la faille, mise à jours rapide de son implémentation logicielle)
- Les médias et assimilés (explications de la faille, débats sur les causes, conséquences et enjeux de celle-ci, etc.)
- Les utilisateurs finaux (signalement de préférence en choisissant les services marchands qu'ils utilisent)

Relations d'interdépendance entre tous les acteurs - les développeurs seuls ne peuvent résoudre la crise même s'ils ont un rôle prépondérant ⇒ c'est les autres acteurs qui peuvent mettre à jours leur logiciel.

Coopération sociale reposant sur des réseau sociaux + du capital culturel + une proximité géographique ⇒ présence de en confiance (il y en a) !

Des représentations de ce que doit être la monnaie (optimisation vs modification des règles consensuselles)

Système pensé comme étant résilient aux failles. Pour autant, l'humain doit intervenir pour les repérer et les résoudre = relation on chain + hors chaîne ⇒ diversité des intermédiations.

Conclusion :

Une structure de gouvernance doit être en mesure de définir :

- le statut de ses membres et les modalités de leurs participations
- des objectifs collectifs et des modalités de contrôle de ses résultats (évaluation, sanction)
- de gérer et de trouver des solutions pacifiques aux conflits
- de contrôler les relations de pouvoir et
- d'asseoir la légitimité des règles qu'elle crée ou modifie.

Contrairement au récit de certains de ses promoteurs, **la gouvernance de Bitcoin n'est pas réductible à sa gouvernance *par* l'infrastructure** :

- Bitcoin est une construction **profondément économique, politique et sociale** et requiert :
  - des formes d'institutions sociales (internes et/ou externes), plus ou moins formelles,
  - des procédures d'expression et de délibération.
  - de préserver la légitimité d'ensemble du système.

⇒ Si **du pouvoir existe au niveau de sous-systèmes** (forge logiciel, forum d'expression, relation contractuelle des utilisateurs de passerelles, etc.), au niveau de l'infrastructure d'ensemble, seule de l'autorité subsiste ⇒ **pas de pouvoir discrétionnaire d'un centre / acteurs sur les autres**

- L'analyse de la gouvernance de Bitcoin se doit d'être multidimensionnelle du fait qu'elle est distribuées et polycentrique et relève d'une grande diversité d'acteurs, de relations et dispositifs.
- **Une gouvernance dynamique et évolutive :**
  - **Les équilibres ne sont pas donnés une fois pour toute, ils sont fragiles et peuvent être remis en cause**
    - **Risque de capture par un/des acteurs**

Merci à tou.te.s !

QUESTIONS?

Vous pouvez me joindre

rolland.mael@hotmail.fr

Twitter : @elmalandr0