

École des Hautes Études en Sciences Sociales

Centre d'Étude des Mouvements Sociaux (CEMS)

Discipline : Économie et Sciences sociales

ROLLAND MAËL

**Au-delà des codes : infrastructure et gouvernance
discrète et polycentrique des cryptomonnaies
Bitcoin et Ethereum dévoilées par leurs crises**

Thèse dirigée par: Ève Chiapello

- | | | |
|------|---|---|
| Jury | 1 | Francesca Musiani, CNRS (Rapportrice) |
| | 2 | Jérôme Blanc, Science Po Lyon (Rapporteur) |
| | 3 | Jézabel Couppey-Soubeyran, Paris 1 Panthéon Sorbonne (Examinatrice) |
| | 4 | Éric Monnet, Ehess et Paris School of Economics (Examinateur) |
| | 5 | Alexandre Mallard, Mines Paris (Examinateur) |

Plan de l'exposé

- 1- Questions de recherche
- 2- Cadre théorique
- 3- Méthodologie et matériaux d'enquête
- 4- Structure de la thèse
- 5 - Trois contributions

Les CM comme objets d'étude

Bitcoin & Ethereum

Capitalisation de marché

= 1.88 trillion de \$; 434 milliard pour Ethereum



Les CM comme objets d'étude

Les Cryptomonnaies :



Moyen de paiement virtuel utilisable essentiellement sur Internet, s'appuyant sur la [cryptographie](#) pour sécuriser les transactions et la création d'unités, et échappant à tout contrôle des régulateurs et des banques centrales. (On dit aussi *monnaie cryptographique*.) [Il existe des centaines de cryptomonnaies dans le monde, parmi lesquelles le [bitcoin](#). Parce qu'elles sont dépourvues de cours légal, les spécialistes privilégient l'appellation *cryptoactifs*.]

LAROUSSE

Les « cryptomonnaies », plutôt appelés « crypto-actifs », sont des actifs numériques virtuels qui reposent sur la technologie de la blockchain (chaîne de bloc) à travers un registre décentralisé et un protocole informatique crypté. Un crypto-actif n'est pas une monnaie. Sa valeur se détermine uniquement en fonction de l'offre et de la demande.

Les crypto-actifs ne reposent pas sur un tiers de confiance, comme une banque centrale pour une monnaie. Il existe à ce jour plus de 1 300 crypto-actifs. Les plus connus sont le bitcoin, le ripple, l'éther, le litecoin, le nem et le dash.

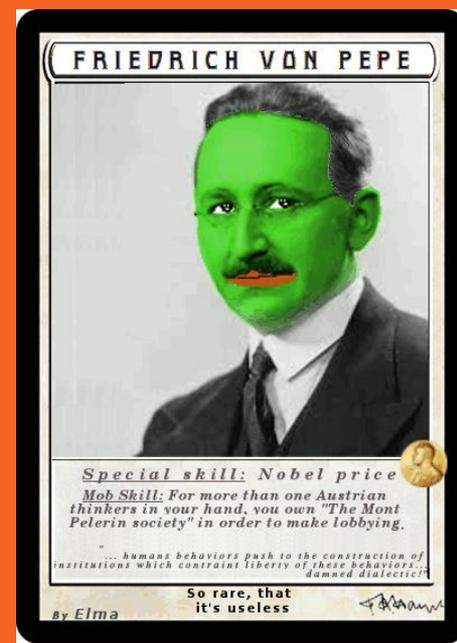
Les CM comme objets d'étude

Bitcoin : une « évolution radicale de la monnaie » (Buterin 2013d) :

“sans confiance”,
“complètement décentralisée”
et “entièrement peer-to-peer,
sans tiers”

(Nakamoto 2008c, 2009b).

Le consensus politique est remplacé par un consensus technique, indiscutable et non négociable.





1- Question de recherche



1- Question de recherche

Le syllogisme des prétentions technicistes

(i) Puisque la technique est autonome et neutre vis-à-vis du monde social

(ii) que les CM sont purement techniques,
alors

(iii) ces monnaies sont immunisées de la gouvernance humaine et de ses intérêts,

en faisant

(iv) de « meilleures » monnaies que les formes monétaires antérieures, en particulier les « monnaies fiat » nationales.



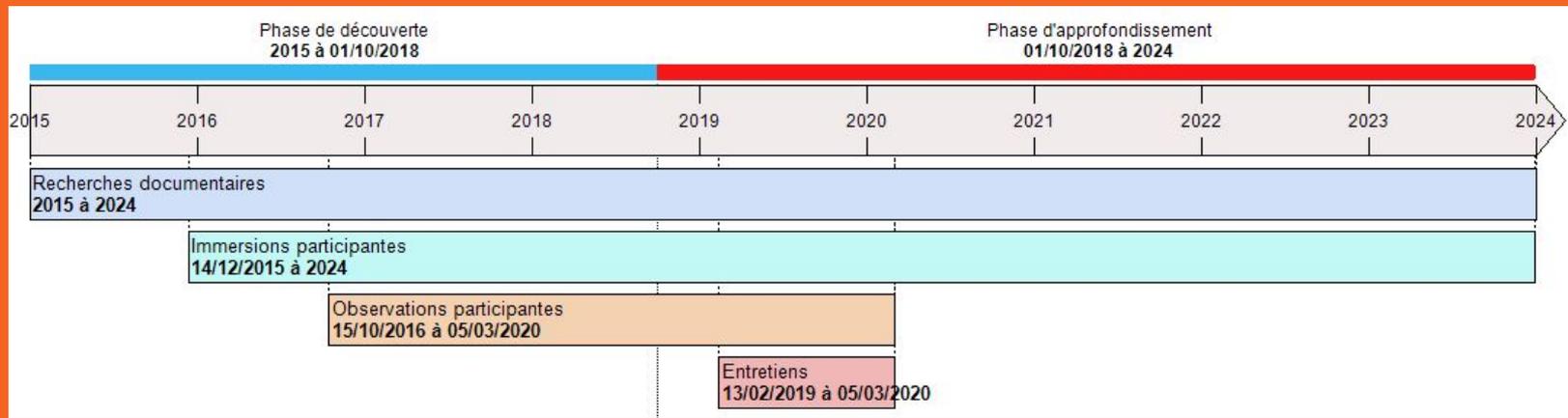
2- Cadre théorique



Institutionnalisme monétaire
francophone

Sociologie des sciences et
techniques, des controverses et
des crises





3- Méthodologie

Une enquête multiniveau et des matériaux hétérogènes:

- Recherches documentaires : n = 661 ; de 2015 à auj.
- Immersion participantes : Indénombrable, de 2016 à auj.
- Observations participantes : n = 28 ; de 2016 à 2020
- Entretiens : n = 27 ; de 2016 à 2020

4- Structure de la thèse

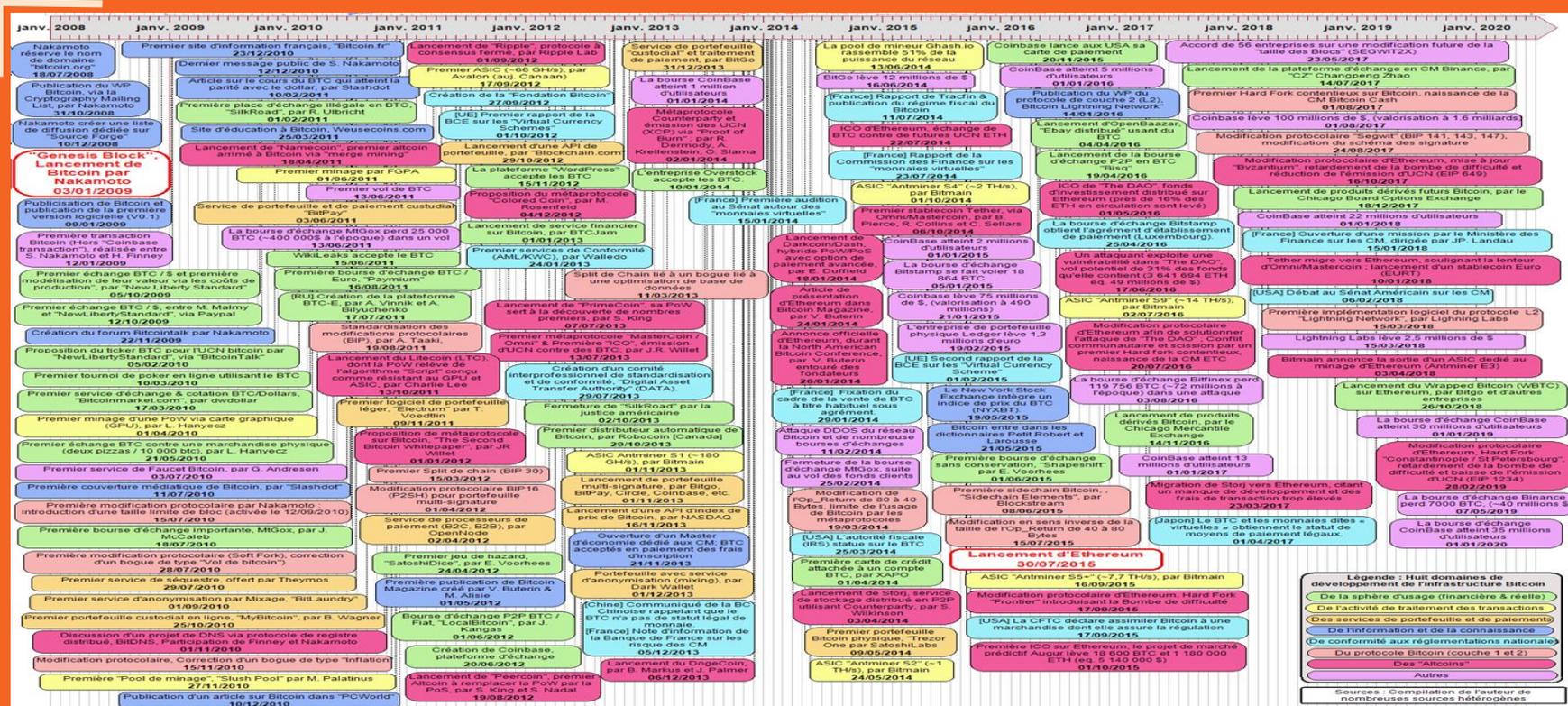
Chapitre I - Une socio histoire de l'émergence carnavalesque des infrastructures Bitcoin et Ethereum

Chapitre II - Une participation critique à la controverse sur le statut monétaire des CM

Chapitre III - Une sociologie des crises de Bitcoin et d'Ethereum pour dévoiler leur gouvernance

5- Contribution 1: aux études infrastructurelles

5- contribution 1: aux études infra-structurelles



Légende : Huit domaines de développement de l'infrastructure Bitcoin

- (De la sphère d'usage (financière & réelle)
- (De l'activité de traitement des transactions)
- (Des services de portefeuille et de paiements)
- (De l'histoire et de la connaissance)
- (De conformité aux réglementations nationale)
- (Du protocole Bitcoin (couche 1 et 2))
- (Des "Altcoins")
- (Autres)

Sources : Compilation de l'auteur de nombreuses sources historiques

5- Contribution 2: à la théorie monétaire institutionnaliste

5- Contribution 2: à la théorie monétaire institutionnaliste

Les Actifs Numériques

Terme valise, non réservé aux UCN des protocoles de registre distribué, il inclut les actifs virtuels, les points de fidélités, etc.

ex: Linden Dollars du jeux second life, la monnaies communautaire Sardex, les tickets restaurant, etc.

Les Crypto-Actifs

Terme valise, incluant les monnaies ou titres émis et circulant dans des protocoles de registre distribués (UCN et tokens).

ex: XRP de ripples, de nombreux tokens émis lors d'ICO, etc.

Monnaie numérique

Terme réservé aux monnaies traditionnelles émises sur des protocoles de registre distribué

Monnaie Numérique de Banque Centrale

Terme réservé aux monnaies nationales émises sur des protocoles de registre distribué

Logique fiduciaire du sceau

ex: Central Bank Digital Currencies.

Monnaie Numérique privée

Terme réservé aux monnaies privées émises sur des protocoles de registre distribué

Logique contractuelle de signature

ex: Tether, etc.

Les Crypto-Monnaies

Terme réservé aux UCN émises par des protocoles de registre distribué ouverts

Logique fiduciaire de consensus distribué

ex: Bitcoin, Ethereum.

5- Contribution 3 : à la sociologie des crises

5- Contribution 3 : à la sociologie des crises

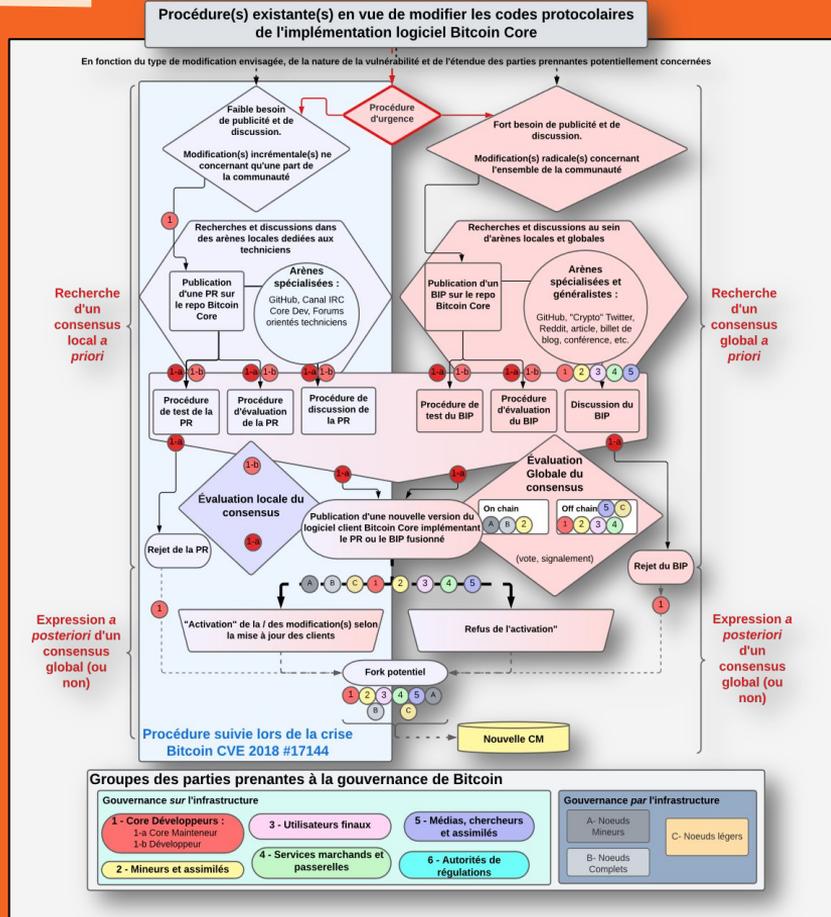
Tableau 5 : Les deux grandes familles de crises protocolaires

...ce qui est attendu = considéré comme légitime par le consensus social
 ...ce qui n'est pas attendu = considéré comme illégitime par le consensus social

<p>[a] Situation normale</p> <p><u>Action : Statu quo</u></p> <p>Ex. : <i>contrôle de la double dépense, création monétaire qui suit l'échéancier prévu, etc.</i></p>	<p>[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>Ex. : <i>double dépense et régulation de la création monétaire suivant les règles et l'échéancier prévu (Cas CVE 20182).</i></p>
<p>[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>Ex. : <i>SegWit et le Scaling Debate; The DAO hack.</i></p>	<p>[d] Situation normale</p> <p><u>Action : Statu quo</u></p> <p>Ex. : <i>rejet des doubles dépenses, invalidation de toute création monétaire qui ne suit pas les règles et l'échéancier prévu, etc.</i></p>

Le code permet ...

Le code ne permet pas...



5- Contribution 3 : à la sociologie des crises



Je vous remercie pour votre attention

