Monnaies locales et Cryptomonnaies: Quel avenir?

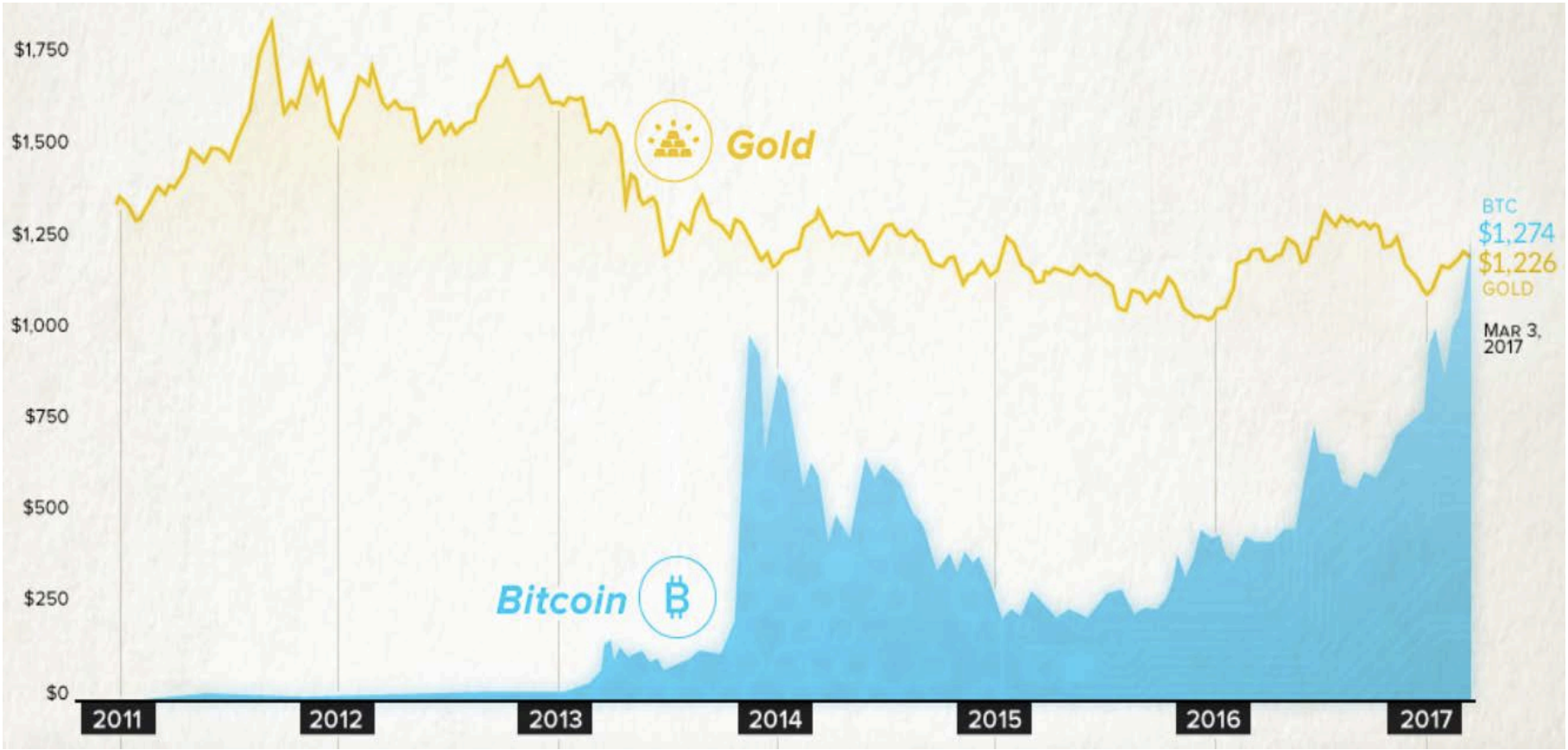
Odile Lakomski-Laguerre

Printemps de l'économie, 6ème édition, mercredi 21 mars 2018

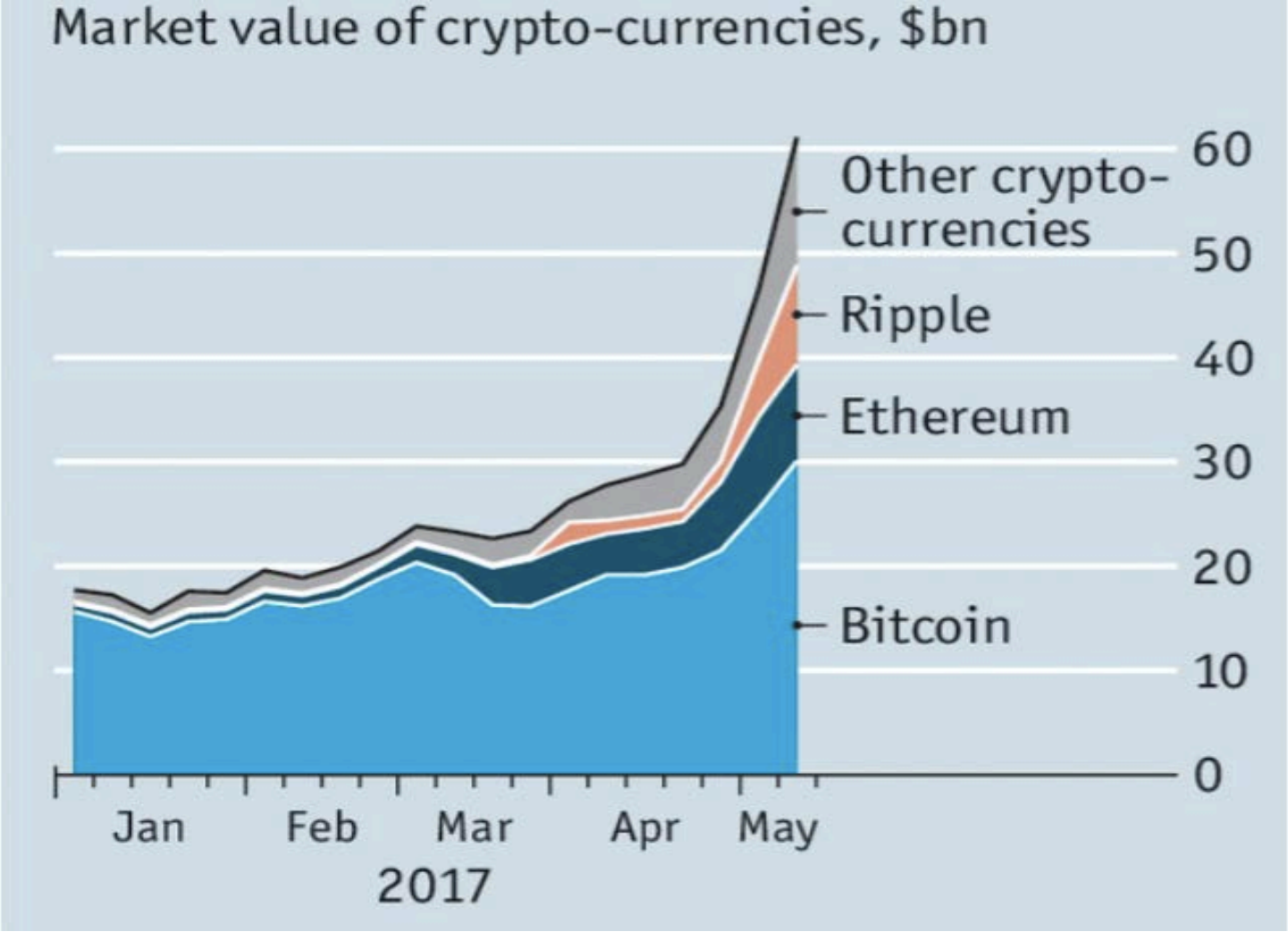
O. Lakomski-Laguerre, Université de Picardie Jules Verne (CRIISEA)
L. Desmedt, Université Bourgogne - Franche Comté (LEDI)

Introduction

Fin 2008, Bitcoin : proposition sur mailing list de cryptographes.
novembre 2009 : 1btc = 0,01 USD ; juin 2017 : 2900 USD



Autres cryptomonnaies : Ether (2015), Ripple (2012), Litecoin (2011), Dash (2014), Monero (2014)…



Introduction

A partir de 2011-2012 : « ruée" analytique sur le phénomène Bitcoin, avec plusieurs niveaux de discours :

- ✓ Soit opposition binaire entre partisans et critiques
- ✓ Soit approches multiples (informatique, droit, économie, sociologie etc.).
- ✓ Mais pour la grande majorité de travaux : aucune analyse théorique de la monnaie ; pas de retour sur le ***concept*** de monnaie

Bitcoin / monnaies cryptographiques :

- ✓ **Nouvelle ère dans l'histoire monétaire**? (Monnaie métallique ➔ Monnaies fiduciaire et scripturale bancaire ➔ Monnaie électronique)
- ✓ Emergence de systèmes de paiements concurrentiels = **fin d'une conception unitaire de la monnaie** ?
- ✓ Emergence des monnaies de réseau (Internet) = **monnaies complémentaires** dans une économie mondiale en crise?

Introduction

« *When I asked a Bitcoiner about the theory of money underlying his understanding of cryptocurrency, he compared Bitcoin to gold* », Dodd, 2015.
Caractéristiques du Bitcoin, selon Dodd :

- le réseau serait « plat » (*flat*), sans hiérarchie
- offrirait des solutions technologiques aux problèmes de gouvernance (inflation)

- rendrait superflue la **confiance** entre échangistes
- Bitcoin serait une « monnaie sans dette », à l'instar de l'or (actif "naturel")

-> Perspective institutionnaliste

- ✓ La monnaie comme institution sociale : ensemble de règles destinées à organiser les paiements
- ✓ Historicisation de la monnaie : les formes historiques correspondent à des modèles économiques (idéaux-types?)
- ✓ Articulation entre pratiques monétaires (éco) et ordre monétaire : les valeurs du réseau BTC
- ✓ Confiance et légitimité de la monnaie

Introduction: plan

1) L'innovation technologique

- Contexte d'apparition ; blockchain ; nouvelle monnaie ou nouvel actif spéculatif ?

2) Le monnayage : entre nouveauté et vieux débats

- Argument : « libérer la monnaie de l'Etat » ; un retour au métallisme ? ; de nouveaux principes de monnayage ?

3) Confiance et légitimité du système BTC

  - Pose la question des modes de coordination spécifiques aux cryptomonnaies

1) Bitcoin et blockchain, nouveautés technologiques

Le Bitcoin: quelle innovation ?

- Ce n'est pas le caractère "virtuel", "digital" : depuis les années 1970, monnaie majoritairement électronique, numérique

- Monnaie cryptographique
  - ✓ Un langage, une culture particuliers (algorithmes, informatique, *open source*…)
  - ✓ Anonymat : respect des données privées

- Décentralisation, désintermédiation
  - ✓ Pas de tenue des comptes centralisée
  - ✓ Fonctionnement en réseau "*peer to peer*" (validation et contrôle des transactions) ➔ aucun nœud de calcul dominant

1) Bitcoin et blockchain, nouveautés technologiques

Présentation rapide du système

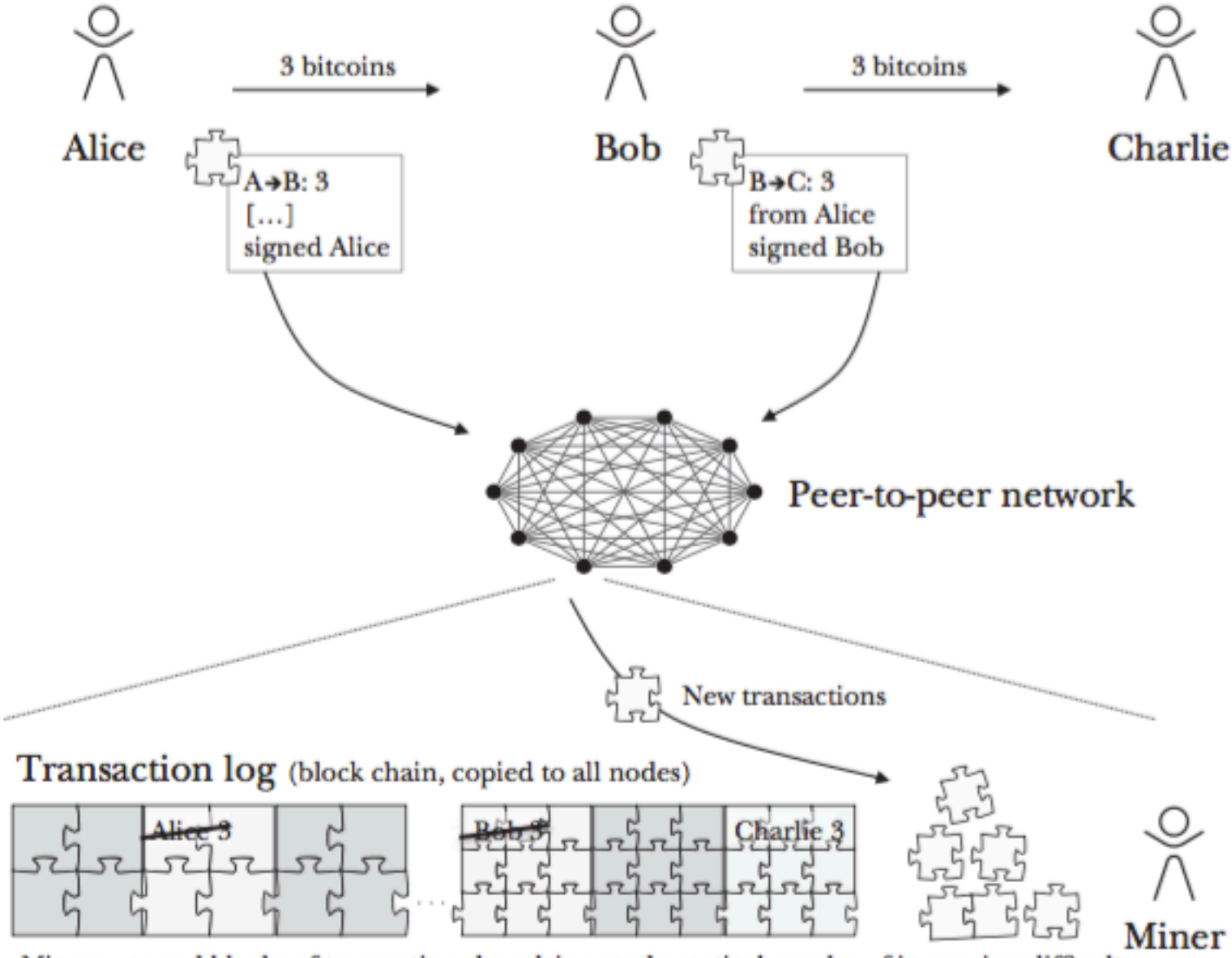
✓ Définition d'une unité de compte : le btc

✓ Pas de procédure de règlement des soldes. Support : porte-monnaie virtuel (suite de chiffres et de symboles, associé à une paire de clés privée et publique)

✓ Le Bitcoin est une technique de transfert de messages, d'informations codées (dont la monnaie est une application particulière), qui repose sur :

- **Cryptage** : cryptographie asymétrique
- **Minage** : communauté organisée en réseau qui valide et authentifie les transactions
- Technologie de la ***Blockchain*** : journal public qui regroupe chronologiquement toutes les transactions effectuées dans le réseau depuis le début

Bitcoin's Approach to Transaction Flow and Validation



Miners append blocks of transactions by solving mathematical puzzles of increasing difficulty.

Monnaie ou actif spéculatif?

Le Bitcoin présente **théoriquement** les caractéristiques d'un SP : unité de compte, règles d'émission et de circulation etc.

Mais : **ambivalence entre monnaie (unité de compte et moyen de paiement) et actif (réserve de valeur et instrument de spéculation).**

- Le système semble être actuellement dominé par une vision de la monnaie comme marchandise, actif évaluable par le marché
- Bulle spéculative, valorisation et volatilité : entre en conflit avec la fonction d'unité de compte

2) Théories anciennes et nouveaux principes

Projet lancé en pleine crise financière: Bitcoin clairement présenté comme une alternative aux dérives des institutions financières.

S. Nakamoto : "*The root problem with **conventional currency** is all the **trust** that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve*"

(Nakamoto, 2009, P2P Foundation)

➔ Premier bloc de BTC encodé avec le message suivant:

"*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*"

2) Théories anciennes et nouveaux principes

« Libérer la monnaie de l'Etat »

- **Influence du mouvement crypto-anarchiste** : en 1985, D. Chaum, cryptographe et cypherpunk lance l'idée de monnaie cryptographique dans "*Security without identification: Transaction Systems to make Big Brother Obsolete*

➔ utilisation de la cryptographie pour protéger la vie privée (notamment vis-à-vis des gouvernements)

- **Influence de l'école autrichienne** : BTC récupéré par les tenants des approches libérales

➔modèle de concurrence monétaire à la Hayek ?

1976 : Hayek, *Denationalisation of money*

2013 : le *Mises circle* (Université du Texas) créée le *Satoshi Nakamoto Institute*

2015 : Hayekgold

Pourtant chez Hayek les monnaies sont émises par des **banques…**

2) Théories anciennes et nouveaux principes

- Un retour au métallisme ? « *coins* », « minage »
- Plafonnement de l'émission. « Rareté absolue », Selgin :

Figure 1: Base Money Types

		Nonmonetary Use?	
		Yes	**No**
Scarcity	**Absolute**	Commodity	Synthetic Commodity
	Contingent	Coase Durable	Fiat

- Monnayage :«*Money is created when a stakeholder uses its singular location at the hub of a community to mark the disparate contributions of individuals in a common way*» (Desan, 2014).

➔Historiquement : Hôtels des monnaies, banques. Aujourd'hui : réseaux

3) Le Bitcoin comme ordre monétaire cohérent ?

Perspective institutionnaliste :

Question centrale de la confiance dans la monnaie / Légitimité des institutions monétaires (Cf. Aglietta et Orléan (1998), B. Théret (2008)…)

Les formes de la confiance :

- Confiance **méthodique** : ancrée dans les pratiques régulières d'échanges par la répétition des relations marchandes

- Confiance **hiérarchique** : Celle que l'autorité politique imprime à la monnaie ; l'autorité politique sur la monnaie a le pouvoir de changer les règles

- Confiance **éthique** : Conformité des politiques de la monnaie à un ordre monétaire (valeurs et adhésion du public).

La confiance selon Bitcoin

- "*What is needed is an electronic payment system based on cryptographic proof instead of trust*" (Nakamoto, 2009)

➔ Ambivalence vis-à-vis de la notion de confiance :

- ✓ le codage **plutôt** que la confiance
- ✓ le codage comme **gage** de confiance ?

- Bitcoin.org « La cryptographie est une branche des mathématiques qui permet de créer des preuves mathématiques qui offrent un haut niveau de **sécurité** »

Formes de confiance et crypomonnaies : les contradictions

Confiance Méthodique :

- blockchain, minage et cryptographie
- garanties contre la contrefaçon, traçabilité

Problèmes

- robustesse du réseau
- mais faiblesses de l'écosystème BTC: fraudes, faillites (Mt gox 2014…), piratage des portefeuilles

Formes de confiance et crypomonnaies : les contradictions

Confiance Hiérarchique : le code source fait autorité

- protocole et règles établis par Nakamoto
- communauté sans leadership

Problèmes

- Quelle gouvernance? Qui décide de changer les règles?
- Conflit récent sur la taille des blocs : les *hardforks*

Formes de confiance et crypomonnaies : les contradictions

Confiance éthique :

- techno-libertarisme
- anonymat et transparence
- Décentralisation et nouveaux communs

Problèmes :

- **Anonymat :** modèle éthique et commercial du BTC pour la communauté d'origine (crypto-anarchistes), **mais**
  - ✓ le BTC n'est pas vraiment anonyme
  - ✓ réputation sulfureuse du BTC (difficile pour le grand public)
- Le BTC n'est pas un système vraiment décentralisé : concentration pour les principaux acteurs de l'écosystème(minage, plateformes d'échanges etc.)
- Reproduction des tares de la monnaie capitaliste : accumulation, spéculation

Conclusion

- **Le Bitcoin : Une vision procédurale de la monnaie**
  - Retour à la théorie de la monnaie marchandise?
  - Revanche des idées autrichiennes?
  - L'hypothèse de la monnaie comme institution est-elle encore valide?
- **Le Bitcoin : une configuration plutôt inédite**
  - Coexistence avec le système monétaire officiel : une nouvelle devise internationale
  - Dans l'univers des cryptomonnaies : offre concurrentielle de monnaie
  - Multiplicité de la monnaie

  ➔ Complexe pour la théorie
- **Faire une théorie appropriée du BTC** : nouveau langage? Nouveaux concepts (théorie informatique)?