L'alternative Bitcoin : Une lecture théorique à partir de l'institutionnalisme monétaire

Odile Lakomski-Laguerre
Université de Picardie Jules Verne

Introduction

- **Dans les années 1980 : mutation des systèmes financiers et 1ère vague d'innovations financières**
  - NTIC et développement de la finance de marché, libéralisation
  - Nouveaux produits financiers
  - Ouverture de nouveaux marchés : dérivés

- **Plus récemment (surtout après 2008) : nouvelle vague d'innovations financières mais aussi *monétaires***
  - Dans le domaine de la finance : Fintech, trading haute fréquence, plateformes de crowdfunding etc.
  - Dans le domaine monétaire :
    - ✓ Monnaies locales et complémentaires (avec une vocation ESS)
    - ✓ Nouveaux modes de paiement : sans contact, mobile money
    - ✓ Nouveaux services de paiement
    - ✓ **Nouvelles formes monétaires : cryptomonnaies**

Introduction

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?

➢Le potentiel d'innovation de ces monnaies est-il susceptible de **révolutionner les questions monétaires et financières**?

- ✓ **Véritable nouveauté?**
- ✓ **Ou bien résurgence de vieux débats théoriques?**

➢Dans l'histoire des idées, le changement d'une forme de monnaie à une autre s'est toujours accompagné d'un **retour sur la question de la nature de la monnaie**

Cf. (débats Bullionnistes/Anti-bullionnistes, Currency/Banking School au 19ème ; débats Métallistes/Nominalistes début 20ème)

Introduction

Bitcoin avec une grille de lecture théorique : une perspective institutionnaliste

Hyp: La monnaie est une institution sociale = un ensemble de règles destinées à organiser les échanges marchands

Cela suppose:

✓Articulation entre logique d'un système de paiements (relève de l'analyse éco) et institutions de la société (socio-éco) : pose la question des **valeurs** et des **influences idéologiques** du réseau BTC

✓Notions centrales de **confiance** et **légitimité** de la monnaie

Plan

1.L'alternative Bitcoin : rupture technologique, influences et valeurs

- **Le BTC n'est pas une technologie neutre** : derrière l'apparente "froideur" des maths et du code, il y a un ensemble de valeurs et une idéologie de la monnaie, qui se posent comme alternative à un ordre monétaire correspondant à un modèle de capitalisme fondé sur la collusion Banques-Etats

2.Monnaie complémentaire ou nouvel ordre monétaire?Confiance et légitimité du système BTC

- Support du développement d'un objet monétaire : la confiance
- Pose la question de l'organisation des communautés BTC et autres cryptomonnaies, de leur gouvernance

Présentation rapide du système

✓Définition d'une unité de compte : le btc

✓Monnaie équivalente à de l'argent liquide : 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 (système d'horodatage)

1. L'alternative Bitcoin (1) : quelle rupture?

Bitcoin Mining : Processus d'enregistrement (validation et authentification) de nouvelles transactions dans la blockchain

➔ Mettre au service du réseau de la puissance de calcul : résolution de problèmes mathématiques complexes

➔ **Système d'incitations** : Rétribution des mineurs en échange d'une « *proof of work* » (25 btc aujourd'hui ; 12,5 été 2016).

➔ **Auto-régulation** du système : plus il y a de mineurs dans le système, plus le minage est difficile et la contrefaçon ardue. Conséquences :

- ✓ Contrainte de rentabilité (coût d'acquisition du matériel versus rémunération en BTC)
- ✓ Le minage est passé à un **stade industriel** : concentration en "pools" de mineurs ("fermes" de minages). « Problème des 51% »
- ✓ **Dépense énergétique et coût environnemental** : les fermes de minage se concentrent dans des zones où l'électricité est peu onéreuse ➔ En **Chine** principalement.

1. L'alternative Bitcoin (1) : quelle rupture?

- **Quelques statistiques (11 novembre 2017)**
  - 16,67 millions : l'offre de Bitcoins actuelle. Notez que l'offre totale est limitée à 21 millions de Bitcoins, et que le dernier Bitcoin sera émis en mai 2140 (si le réseau existe toujours).
  - 55% : la domination du Bitcoin sur le marché des crypto-monnaies.
  - 4,9 milliards de dollars : le volume d'échange sur 24 heures.
  - 96 : le nombre de pays dans lesquels le Bitcoin peut-être utilisé librement.

1. L'alternative Bitcoin (1) : quelle rupture?

Le Bitcoin: quelle innovation?

•Le Bitcoin est une combinaison ingénieuse de technologies qui existaient déjà : cryptographie, logiciels open source, réseaux p2p et internet, consensus distribué

- ➢ Mais Satoshi Nakamoto (2009) résout un problème essentiel bien connu en informatique : le problème dit des "Généraux Byzantins"

• L'innovation n'est pas dans le caractère **"virtuel", "digital" :**

– La monnaie est fondamentalement abstraite (unité de compte)

– La monnaie bancaire est elle aussi numérique (informatisation des opérations)

- ➢ **Toute monnaie repose aujourd'hui sur des supports informatiques (ordinateurs, smartphones)**
- ➢ **Il y a de la matérialité derrière le BTC (le minage) : infrastructures de réseaux, cables, fibre optique, électricité, systèmes de refroidissement etc.**

1. L'alternative Bitcoin (1) : quelle rupture?

En quoi est-ce différent?

- **Décentralisation, désintermédiation**

✓Pas de tenue des comptes centralisée

✓Fonctionnement en réseau "*peer to peer*" (validation et contrôle des transactions)

✓Disparition des tiers de confiance

- **Monnaie non bancaire (et *anti-banques*)**

✓La création de monnaie ne se fait pas en contrepartie du crédit

✓Alternative à un capitalisme fondé sur crédit ?

- **Pas de souveraineté étatique**

✓Monnaie transnationale

✓Echapper au contrôle de l'Etat et se réapproprier la monnaie (notion de communs)

- **Une innovation sans visage**

✓Mystère autour de l'identité de Nakamoto

✓De l'entrepreneur individuel schumpétérien à la communauté

1. L'alternative Bitcoin (1) : quelle rupture?

Une monnaie anti-banques : Le projet est lancé en plein contexte de crise financière:

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)

➢**Contestation très forte de la monnaie actuelle :**

- ✓ Crises bancaires et financières
- ✓ Pouvoir monétaire concentré dans les mains des grands groupes bancaires
- ✓ Dette publique

➢**Contestation d'un capitalisme fondé sur la collusion Banques/Gouvernement**

1. L'alternative Bitcoin (2) : Influences et valeurs. Utopie libertarienne d'un monde sans Etat?

1/ Mouvement Cyberpunk et Cryptographes anarchistes :

- Mouvement Cyberpunk : romans de Neal Stephenson

Cypherpunks Mailing list (la plus active entre 1992 et 2001) = regroupe des hackers, cryptographes et défenseurs de la vie privée ➔ utilisation de la cryptographie pour protéger les données privées

- Cryptographes anarchistes et monnaie intraçable
  - **D. Chaum** = Idée de monnaie cryptographique *Digicash* (anonymat et non-traçabilité) pour échapper au contrôle étatique (1985)
  - **Wei Dai** = propose la monnaie électronique b-money en 1998.
  - **Nick Szabo** = développe en 1994 une théorie des contrats numériques, puis entre 1998 et 2005 il travaille au projet d'une monnaie numérique en ligne BitGold

Les valeurs : Anonymat, liberté individuelle, respect des données privées (/ Etat ou grandes entreprises telles les GAFA)

2/ Défense du marché libre : lectures autrichiennes/libertariennes

➔ Discours officiel des promoteurs du BTC : promotion des libertés individuelles, BTC comme devise globale, commune, anonyme.

➔ Bitcoin n'est pas la seule monnaie cryptographique : Foisonnement d'innovations monétaires et multiplicité des monnaies virtuelles (car logiciel *open source*). On répertorie aujourd'hui environ 1000 monnaies cryptographiques / Les plus importantes : BTC, Ether, Ripple

F.A. Hayek, *Denationalisation of Money,* 1976 :

•Libéralisme et souveraineté de l'individu

•Recherche d'une monnaie non inflationniste, saine (exempte de manipulations politiques)

•Nouvel ordre monétaire fondé sur les vertus de la concurrence

➔ BTC récupéré par les tenants des approches libérales d'inspiration autrichienne

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

Retour à la "naturalisation" de la monnaie : un “métallisme digital” ? (Maurer, Nelms, Schwartz, 2013)

- **Références explicites à la monnaie or :**
  - ✓ Termes employés (*Coins, mining, diggers*… "or numérique") :

*"Bitcoin mining is so called because it resembles the mining of other commodities: it requires exertion and it slowly makes new currency available at a rate that resembles the rate at which commodities like gold are mined from the ground"*https://en.bitcoin.it/wiki/Mining

✓Or = symbole universel, sain, valeur refuge (objectif monnaie internationale)

Greenspan, 1966 : *“Gold stands as a protector of property rights”*

- **“Métallisme pratique" (Schumpeter 1954) :**
  - Offre limitée de BTC : plafonnement de l’émission
  - Retour du débat : **Rules *vs* Discretion** / L'or garde-fou contre les manipulations monétaires : monnaie a-politique

Iconographie très explicite : besoin de représenter une richesse tangible, un travail d'extraction (*Proof of Work*)

Le problème du statut juridique

•Définitions "officielles" de la monnaie électronique:

- ✓ Union Européenne : **Directive communautaire 2000/46/CE du 18 septembre 2000, puis Directive 2009/110/CE du 16 septembre 2009** sur la monnaie électronique
- ✓ En France : **article L315-1 du Code monétaire et financier**, qui transpose l'article 2.2 de la directive 2009/110/CE. Monnaie électronique = "*valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur (…) et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique*"

•Autorités publiques, juridiques : le BTC n'est pas une monnaie

- ✓ Pas de cours légal (de fait, pouvoir libératoire limité)
- ✓ Le réseau qui l'émet n'a pas la statut légal d'établissement de crédit

•Commission des finances du Sénat 2014 : table ronde sur le statut juridique du BTC

- ➢ Difficulté à appréhender la monnaie cryptographique
- ➢ Aucune législation spécifique adoptée à ce jour en France

•Réflexions sur le sujet plus avancées dans d'autres pays : Alle, GB, USA et Canada

Le BTC est-il une monnaie?

OUI…

➢ **Le Bitcoin présente théoriquement les caractéristiques d'un Système de Paiements :**

- ✓ unité de compte : abstraite, conventionnelle
- ✓ règle d'émission des signes monétaires (déterminée par le code et les algorithmes)
- ✓ Règle de monnayage : en contrepartie de quoi les BTC sont-ils émis? Energie électrique? Puissance de calcul des ordinateurs?

- **C'est aussi une réserve de valeur** : C'est même SURTOUT ça !

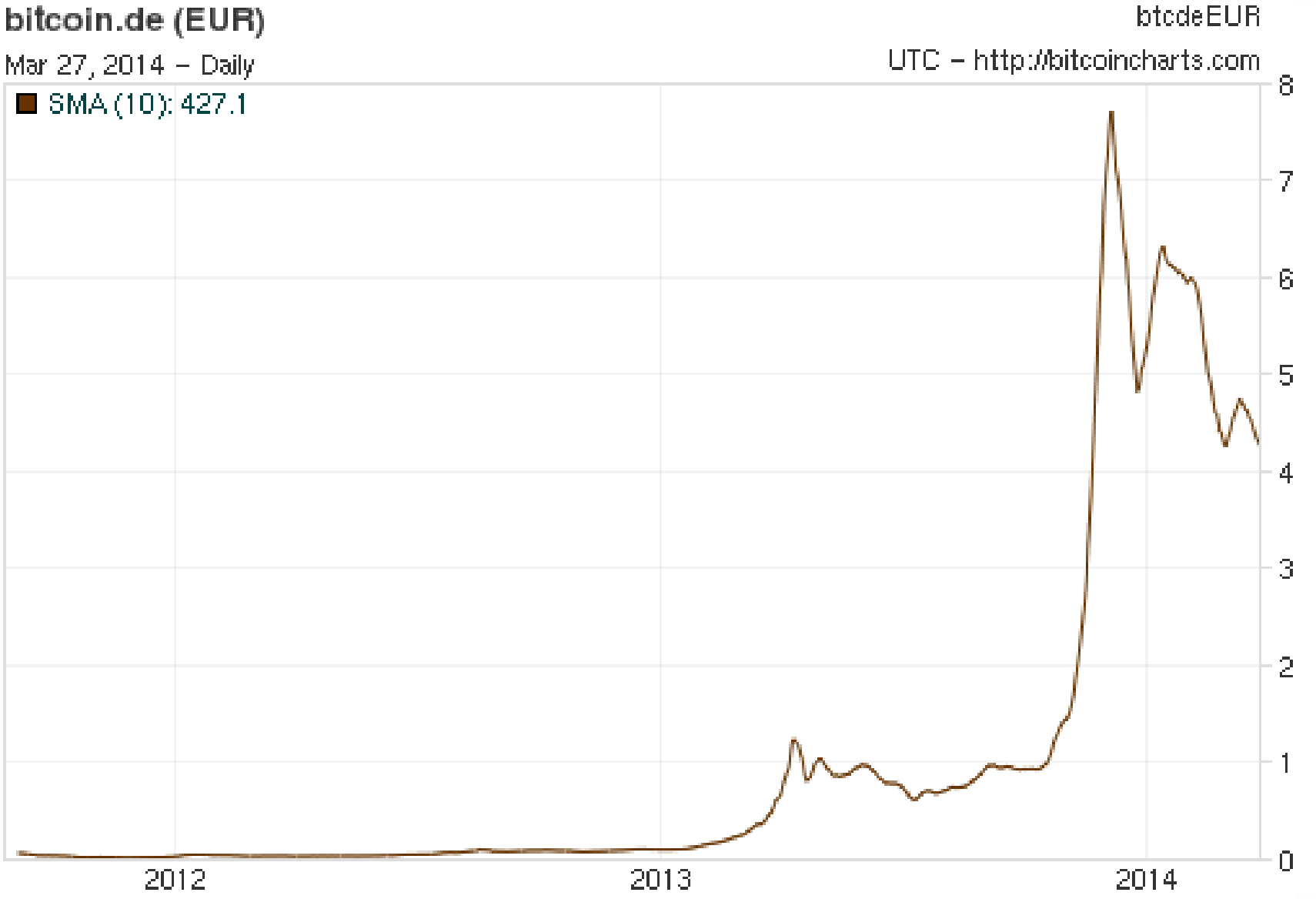
  - Le BTC a été pensé comme cela. L'offre est limitée à terme (21millions de BTC à horizon 2040), et si la demande augmente progressivement… Alors la valeur (pouvoir d'achat de la monnaie) doit nécessairement monter!
  - Système nécessairement déflationniste
  - Conséquence de l'influence des théories qui réduisent la monnaie à une marchandise, un bien

- **…D'où une question majeure : monnaie ou actif spéculatif?**

Bulle spéculative autour du BTC : Cela attire les spéculateurs en quête de nouvelles sources de rentabilité + engouement pour la nouveauté / Comparable à la bulle internet fin 90' début 2000.

- **!!!! Ne pas confondre dans ce cas valeur de la monnaie** (pouvoir d'achat dans son système d'échanges) et **taux de change** du BTC / devises officielles. Ce qui est volatil, c'est le **cours du BTC** comme **devise**.
- **Comment déterminer le cours?** Par la valeur qu'on peut attribuer au "sous-jacent" (le réseau Bitcoin?): Question des fondamentaux et de la déconnexion / fondamentaux
  - Pure activité spéculative alimentée par l'intérêt médiatique (le battage même) pour la monnaie virtuelle : par anticipation d'un attrait pour cette monnaie alternative, des investisseurs auraient acheté en masse du Bitcoin
  - Et comme n'importe quel actif spéculatif = rumeurs, discours etc
  - Forte volatilité du cours : atteint presque 20000 dollars avant Noël 2017 et chute de près de 50% depuis (retombé sous la barre des 10000 le 17 janvier)

2. Monnaie complémentaire ou nouvel ordre monétaire ?
(1) Le Bitcoin est-il une monnaie?



2. Monnaie complémentaire ou nouvel ordre monétaire ?
(2) La confiance

Théories institutionnalistes de la monnaie : la question centrale de la confiance (Aglietta et Orléan 2002, B. Théret 2008…**):**

3 formes de confiance

- **Confiance méthodique** : c'est l'assurance que l'usage de la monnaie va permettre la régularité et la continuité des transactions (acceptation généralisée des instruments d'échange)
- **Confiance hiérarchique** : c'est celle que l'autorité politique imprime à la monnaie (souveraineté) ; elle a le pouvoir de changer les règles
- **Confiance éthique** : renvoie à l'idée de légitimité voire d'idéologie de la monnaie ; idée d'une conformité des politiques de la monnaie à un ordre économique et monétaire (ex: monnaie bancaire de crédit et capitalisme industriel, centralisation monétaire et politique monétaire conduite par la banque centrale)

➢**Une monnaie complète requiert une articulation cohérente entre ces trois niveaux de confiance *:* Il faut que l'utilisation d'une monnaie corresponde à un modèle de société (ensemble de valeurs qui font consensus)**

Ex: l'expansion de la monnaie bancaire de crédit correspondait parfaitement au décollage industriel du capitalisme (modèle de capitalisme théorisé par Schumpeter)

- Le Bitcoin et la question de la confiance

  Nakamoto, 2009 :

  "*What is needed is an electronic payment system* ***based on cryptographic proof instead of trust***"

- une certaine **ambivalence** vis-à-vis de la notion de confiance :

  le code informatique **plutôt** que la confiance ou le code au fondement de la confiance ?

Le Bitcoin et la confiance méthodique :

➢**Pour ancrer la confiance : cryptographie (infaillibilité des maths et des algorithmes), réseau et consensus distribué (pas de manipulation au profit d'un pouvoir central), transparence (registre accessible à tous)**

•**Depuis 2009, le protocole fonctionne** (ne pas confondre robustesse du protocole et fragilités dans l'écosystème) :

- blockchain et cryptographie robustes : Aucune attaque de type 51% pour l'instant
- Une communauté de développeurs qui semble depuis le début oeuvrer pour la pérennité du système

•**Mais :**

- Problèmes sur les plateformes d'échange : piratages, faillites, fraudes (MtGox 2014, plus récemment Corée du Sud)
- Sécuriser son portefeuille pour éviter les piratages
- Complexité technique, langage d'informaticiens : peut rebuter, sentiment d'un objet compliqué d'utilisation

ET : problème d'engorgement du réseau du fait d'un nombre croissant d'utilisateurs ➔délais de validation des transactions plus longs et nécessité de payer des frais plus élevés pour un traitement rapide (contraire à l'argument de départ, peu de coûts de transaction)

Le Bitcoin et la confiance hiérarchique

➢Règles d'émission et politique monétaire (offre) : code et algorithmes

•Question du statut légal, juridique : garanties pour l'utilisateur?

- ✓ Légitimité de la communauté BTC?
- ✓ Réseaux P2P comme nouvelles formes d'organisation politique?
- ✓ Code is Law?
- ✓ Qui décide? Qui modifie les règles? Derrière les algorithmes et le code, il y a des développeurs, une communauté etc !!

•C'est toute l'ambition du BTC ! Faire glisser la confiance des utilisateurs des institutions vers les blockchains et les réseaux

Le Bitcoin et la confiance éthique

➢**Cohérence entre le fonctionnement de la monnaie et les valeurs qui font consensus à un moment donné**

- **BTC comme promesse de dépassement d'une forme de capitalisme**
- **Blockchain et grandes transitions (économiques, politiques, sociétales)**
  - ✓ Plus de démocratie
  - ✓ Retour aux "communs" : la monnaie en est un
  - ✓ Plus de transparence (Wikileaks etc.)
  - ✓ Transition écologique

➢**Or quelques problèmes et contradictions dans le système BTC :**

1/ Une monnaie anti-capitaliste

- ✓ Offre inélastique : Nouveaux modes d'échange et de consommation? Economie collaborative? Décroissance?
- ✓ Réseaux p2p et revendications communautaires (retour aux "Communs", démocratisation de la monnaie etc.)
- ✓ Nouvelle monnaie et transition écologique

➢ **Valeurs affichées qui se heurtent à :**

- ✓ une idéologie individualiste
- ✓ le BTC est critiqué car il reproduit les tares d'une monnaie capitaliste : thésaurisation, spéculation, enrichissement d'un petit nombre etc.
- ✓ Pb des dépenses énergétiques du minage!
- ✓ Concentration de la richesse sur une minorité de portefeuilles

2/ La communauté Bitcoin

- **Division de la communauté :**
  - ✓ entre ceux qui croient au développement de la monnaie et à un nouvel ordre monétaire, et ceux qui n'y voient qu'un simple investissement purement spéculatif
  - ✓ Sur la question de la taille des blocs : créations de "forks"
- **Profil de l'utilisateur type de BTC** : un homme, environ 30-35 ans, plutôt classe favorisée !
- **Pb d'absence de leadership identifié** : gouvernance de BTC peu transparente
  - ✓ Nakamoto se retire après 2010
  - ✓ Gavin Andresen s'est éloigné après un différend avec d'autres développeurs de Bitcoin Core (refus de le suivre sur ses propositions concernant la taille des blocs)
  - ✓ A comparer avec Ethereum : Vitalik Buterin, leader identifié clairement, communauté de développeurs dynamique etc.

3/ Une monnaie décentralisée ?

- Problème de la concentration des fermes de minage (en Chine surtout) : le BTC appartient-il vraiment à tout le monde?

4/ L'image sulfureuse de la monnaie : Anonymat, fraude et transactions de produits illicites (drogue etc.)

- ✓ darknet,
- ✓ économie parallèle, illégale, financement d'activités criminelles etc.

(Ex cyber-attaque mondiale / rançon en BTC)

… Et le cash alors?

- ➔ Faux débat ?
- ➔ Mais Absence de garanties légales : viabilité d'instruments de paiement a-étatiques ?
- ➔ **Eternelle question du statut juridique (enjeux de fiscalité), à moins que la population ne soit prête effectivement à se passer de l'Etat?**

En guise de conclusion… (1) Perspectives :

BTC comme nouveau Système de Paiements : utilisation encore limitée:

- Difficile de vivre au quotidien uniquement avec des BTC
- Des limites techniques : les langages informatiques de script utilisés pour BTC sont plus restrictifs que ceux utilisés pour Ethereum
- Mais le réseau s'étend et le potentiel est important : populations qui n'ont pas accès à un compte en banque (pauvreté, interdictions etc)

Menaces :

- Pression des milieux bancaires pour freiner la menace?
- Autres monnaies cryptographiques concurrentes (mais le BTC reste dominant)
- Guerre de l'image et de la communication? Diabolisation du BTC, renvoi à son image de monnaie pour les activités frauduleuses, illicites.
- **Le régulateur qui souhaiterait freiner l'expansion du BTC** : réflexions en cours, propositions de règlementation etc (durcissement des positions des autorités notamment en Chine, Corée du Sud)

En guise de conclusion… (2) Perspectives :

Logiciel *open source* : récupération de la technologie blockchain pour d'autres services ?

Mille et une applications possibles de la blockchain : Glissement radical dans l'analyse = **dissociation Bitcoin** (pas d'avenir, pas d'intérêt etc.) **et Blockchain** (hype! Prometteur etc.)

- **Ethereum** et les smart contracts
- **Finance, Assurance, Energie, Actes notariés, système de votes**
- **Autres projets de monnaies cryptographiques (plus solidaires)**

  Ex: Faircoin et Faircoop (Enric Ducan)
- **Les banques récupèrent la technologie**
  - Rationalisation des paiements
  - Baisse des coûts de fonctionnement
- **Blochains privées / Blockchain publique : nouveau débat**
- **ICO : levées de fonds en BTC ou création de "tokens"**

En guise de conclusion… (2) Perspectives :

- **Pour terminer :**

"Le monde monétaire de demain pourrait ressembler à la concurrence du Moyen Age, avec des devises d'Etat, des cryptomonnaies, des monnaies locales, à la fois rivales et complémentaires. Ce n'est pas parce que c'est difficile à imaginer, et plus encore à réglementer, que cela n'arrivera pas".

JM. Vittori, Le bitcoin, une étape logique de l'histoire monétaire, Les Echos du 17/01/2018.

Quelques références

- Aglietta M. et Orléan A. (2002), La monnaie entre violence et confiance, Paris: Odile Jacob.
- Banque de France (2013) « Les dangers liés au développement des monnaies virtuelles», *Focus*
- Blockchain France (2016), *La Blockchain décryptée – Les clefs d'une révolution*, Paris : Netexplo.
- Cartelier (1996), *La Monnaie*, Paris : Flammarion, coll. Dominos.
- Lakomski-Laguerre O. et Desmedt L. (2015), "L'alternative monétaire Bitcoin : une perspective institutionnaliste", *Revue de la Régulation*, n° 18, automne.
- ECB (2015), *Virtual Currency Schemes – A Further Analysis*
- Iwamura, M., Kitamura, Y. et Matsumoto, T. (2014), , « Is Bitcoin the only Cryptocurrency in Town? Economics of Cryptocurrency and Friedrich A. Hayek », sur SSRN
- Maurer, B., Nelms, T. C., & Swartz, L. (2013), « When perhaps the real problem is money itself!: the practical materiality of Bitcoin », *Social Semiotics*, vol. 23, n° 2, p. 261-277.
- Nakamoto, S. (2009), « Bitcoin: A Peer-to-Peer Electronic Cash System »
- Rochard, P. (2013), « The Bitcoin Central Bank's Perfect Monetary Policy », *The Mises Circle*
- Rodriguez, P. (2017), *La révolution Blockchain. Algortihmes ou institutions, à qui donnerez-vous votre confiance?,* Paris : Dunod.
- Swanson, T. (2014), *The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin*, Creative commons
- Théret B. (2008), "Les trois états de la monnaie. Approche interdisciplinaire du fait monétaire", *Revue Economique*, vol. 59, n° 4, pp. 813-841.