Stratégies & Information

◊Stratégies économiques◊ Cognitique financière◊ Gestion de risques◊ Marchés◊

EDITORIAL

Cette nouvelle mouture de la lettre est désormais plus adaptée à la lecture sur moyens électroniques : tablettes, écrans d'ordinateurs ou même smartphone. L'ancien design datant de 1995 a vécu. L'objet de la lettre est toujours le même : essayer d'éclairer le lecteur sur les évolutions importantes du monde financier et économiques et ne pas s'arrêter aux effets de mode et aux pressions de l'émotion, bien en cours de nos jours, mais généralement mauvaise conseillère. Sans espérer trouver la *ultima ratio* des événements, nous essayons d'en trouver les causes profondes : ainsi de notre article de la lettre de février sur la liaison profonde entre les marchés financiers et le marché du pétrole qui est tombé depuis dans le domaine commun. Lire la suite p.16.

SIGRE PRESSE

SERIE N2 numéro 158

Bitcoins[1] et consensus distribué

Joël Lebidois

Ces dernières décennies, les technologies de l'information nous ont habitués à passer de systèmes d'information extrêmement centralisés à des systèmes qui, au contraire, sont de plus en plus distribués. C'est le cas des réseaux de télécommunication dont les anciennes architectures en étoile ont été remplacées par des réseaux maillés composés de nœuds et de serveurs manipulant des paquets de données et des adresses (Internet).

Lire la suite p.2

Les taux bas sont-ils un piège mortel ?

Andrea Brignone

Les gouvernements endettés n'arrêtent pas de se féliciter des niveaux des taux qui allègent considérablement le service de la dette publique. Les acheteurs de biens immobiliers en font autant, ainsi que toute entreprise ou particulier qui a un projet d'investissement. Il n'y a pas de doute : de nos jours il vaut mieux être emprunteur que prêteur. Et de préférence à taux fixe.

Lire la suite p. 10.

Bitcoins et consensus distribué

suite

C'est aussi le cas des bases de données distribuées dont la situation physique ou géographique n'a plus aucune signification (nuages) et il en va de même pour les traitements de données répartis entre des machines distantes pour accomplir une tâche donnée.

Pourtant, certains services semblent encore résister à cette tendance générale vers l'éclatement des structures centralisées; ce sont tous ceux qui font appel à un *tiers de confiance* dont l'une des principales caractéristiques est d'inspirer *confiance* aux utilisateurs sur la base d'un consensus le plus souvent socio-économique, voire réglementaire. Dans cette catégorie on trouve pratiquement tous les *services bancaires* depuis la tenue des comptes jusqu'aux transactions financières de toutes sortes. On trouve aussi tous les services de *notarisation* assurant l'authenticité et l'intégrité de nombreux actes comme les titres de propriété ou les testaments. On trouve également les registres officiels de conservation des hypothèques, le service du cadastre, les agences nationales des titres sécurisés (immatriculations) etc. Mais le secteur privé n'est pas en reste où, entre autres choses, contrats, comptabilité, auditabilité et sécurité réclament aussi des processus de confiance.

Fondamentalement la mission d'un tiers de confiance consiste à tenir un « grand livre » (*ledger* en anglais) où sont consignées « toutes les choses dont on veut être sûrs et de façon pérenne ». Autrement dit, ce grand livre doit être *fiable et infalsifiable* mais néanmoins aisément *consultable* par les utilisateurs. Comme par principe, ce tiers de confiance assure une fonction centralisée, il présente donc, dans tout système, un point critique de vulnérabilité technique, économique ou politique. Ces dernières années, c'est principalement ce constat qui a amené certains à réfléchir à un concept de « confiance distribuée » qui offrirait donc moins de vulnérabilité, mais pas seulement pour cette raison. En effet, parmi les tiers de confiance les plus importants nous n'avons pas encore parlé des Etats (ou groupes d'Etats) dans leur prérogative régalienne de création et de gestion monétaire. La monnaie fiduciaire (ou monnaie fiat) dont ils ont le monopole a une valeur nominale supérieure à sa valeur intrinsèque et ne vaut donc que par la *confiance* que les citoyens peuvent accorder à ces Etats au travers d'institutions centralisatrices. Dans un esprit libertaire, ce monopole a été contesté par un groupe de scientifiques anonymes connu sous le pseudonyme de Satoshi Nakamoto; il fut à l'origine du premier projet de monnaie virtuelle destiné à s'affranchir de toute autorité de tutelle: le *bitcoin* (BTC).

Le réseau Bitcoin

En 2008 paraissait un « white paper[1] » décrivant les principes du système

[1] Bitcoin : A Peer-to-Peer Electronic Cash System, *Satoshi Nakamoto*

proposé; la première implémentation, le premier bitcoin et les premières transactions virent le jour l'année suivante. En s'appuyant sur Internet pour le transport et sur les PC des clients comme terminaux, Bitcoin est un réseau « pair à pair » (P2P) ouvert à tous, où les transactions financières se font anonymement en bitcoins et directement entre utilisateurs sans aucune autorité centrale régulatrice. Ces transactions sont organisées de telle sorte qu'un bitcoin donné ne peut être en la possession que d'une seule personne à tout instant. Pour assurer que les bitcoins échangés soient affectés aux bons destinataires ou qu'un même bitcoin ne puisse être dépensé plusieurs fois[2], le système construit un grand livre électronique qui rassemble la totalité des transactions depuis la création du premier bitcoin. De par sa construction comme une suite de blocs de transactions vérifiées, cette base de donnée s'est vue attribuée le nom de « blockchain » ou chaîne de blocs et constitue la principale innovation en se substituant au tiers de confiance. Un tel historique permet de prouver qui détient quoi à tout moment. Cette chaîne est fiable car elle est dupliquée et stockée sur les milliers de nœuds que comporte le réseau Bitcoin (environ 8000 nœuds à ce jour). Le contenu de l'historique est infalsifiable grâce un *chaînage cryptologique* des blocs: toute modification d'une transaction dans un bloc invalide la suite des signatures cryptographiques des blocs de la chaîne. Pour obtenir la confiance des utilisateurs il reste encore à garantir l'unicité de l'historique par un mécanisme de *consensus* de ces derniers sur le fait que la blockchain (le grand livre) en cours de construction est bien la bonne et non la création par un ou plusieurs utilisateurs malhonnêtes, à partir de la chaîne originale, d'une chaîne déviante ou « fourche » (fork chain) qui leur permettrait de prendre le contrôle du système. Le problème est d'autant plus ardu que les utilisateurs n'ont aucune raison de se faire confiance, sont anonymes et peuvent entrer ou sortir du réseau à leur grés. Dans ces conditions, il est clair qu'un consensus s'appuyant seulement sur un vote majoritaire des utilisateurs déclarant valable chaque bloc pourrait être mis en échec facilement.

Satoshi Nakamoto a proposé un protocole dit de «preuve de travail[3] ». Chaque nœud est en charge de valider les transactions au fur et à mesure qu'elles sont diffusées à l'ensemble du réseau; c'est en particulier l'occasion de vérifier qu'aucun bitcoin ne fait l'objet d'une double dépense. Chaque transaction approuvée contribue à former le bloc du moment. Le bloc sera à son tour validé par une signature numérique le liant entre autres choses au bloc précédent; mais pour se faire tous les nœuds sont mis en compétition pour résoudre un « puzzle[4] ». Le premier nœud qui y parvient publie alors le nouveau bloc signé qui s'ajoute à la chaîne et il est récompensé par un certain nombre de bitcoins qui sont créés ex nihilo (25 BTC aujourd'hui et création d'un bloc toutes les 10 minutes en moyenne). L'incitation est assez forte pour

[2] Par construction cette menace n'existe pas avec la monnaie fiat – sauf faux monnayage - mais surgit avec toute monnaie virtuelle

[3] Proof of Work (PoW)

[4] Par essais systématiques avec une fonction à sens unique (SHA256), trouver une empreinte (ou hash) du bloc qui soit inférieure à un seuil fixé. Engendre un *nonce* qui est le nombre d'essais réalisés et qui sera la preuve de travail. Le réseau Bitcoin dans son ensemble réalise environ 1 million de tera-hash par seconde (10^{18} hash/s).

pousser tous les nœuds[5] (ou mineurs) à s'équiper des moyens les plus puissants pour résoudre le puzzle ce qui engendre une puissance de calcul totale considérable à l'échelle du réseau. Ainsi, tout attaquant qui veut falsifier un ou plusieurs bloc en créant un « fork » durable devra disposer en moyenne à lui tout seul d'une puissance de calcul au moins égale à 50% de la puissance disponible dans l'ensemble du réseau, puissance qui est elle-même à la limite supérieure des possibilités technologiques du moment[6]. On aboutit ainsi à la réalisation d'un véritable consensus majoritaire qui ne peut être déjoué que par la collusion d'un très grand nombre de « mineurs » ce qui réduit d'autant la probabilité d'une attaque réussie.

Ce sont sur ces bases que le réseau Bitcoin fonctionne depuis 2009 en dépit d'une réputation un peu sulfureuse qui lui a déjà valu quelques déboires entraînant à certains moments une très forte volatilité du BTC face au dollar. Pour mémoire citons le hacking en 2011 de Mt. Gox qui était un point d'échange entre BTC et devises ordinaires ou encore en octobre 2013 la fermeture par le FBI de « Silk Road » qui était un site du « dark net » qui procédait à de nombreuses transactions illégales en bitcoins. Néanmoins, à ce jour (mars 2016) le réseau Bitcoin est encore solide et bien actif:

- Taux de change: 1 BTC = 417 USD
- Nombre total de bitcoins: 15 millions
- Capitalisation totale: 6,2 milliards USD
- Nombre moyen de transactions: environ 2,5/s (VISA: 2500/s)
- Nombre de comptes actifs: entre 3 et 8 millions
- Nombre de nœuds actifs: entre 7 et 8000
- Taille atteinte par la blockchain: 62 GB
-

Problèmes non résolus

Les points qui suivent sont examinés dans l'optique bitcoin mais pour certains d'entre eux peuvent s'appliquer à la plupart des cryptomonnaies.

Problème de gouvernance

Même si un système propose un service décentralisé, il ne peut pas se passer d'une certaine forme de gouvernance au moins au niveau de la maintenance et des inévitables évolutions techniques. Ainsi, tandis qu'une centralisation des décisions techniques devient indispensable, les « développeurs » acquièrent une position nécessairement privilégiée qui pourrait même devenir dominante. Dans le cas de Bitcoin, la cohérence technique du code source (Bitcoin Core) est assurée par une demi-douzaine de développeurs bien identifiés et une communauté de nombreux bénévoles au travers de divers forums et Fondations. Dans le cadre d'une organisation peu contraignante, les processus décisionnels ont du mal à émerger ou conduisent à des tensions entre les divers communautés impliquées: développeurs, mineurs et utilisateurs. L'exemple actuel d'un projet de changement de taille des blocs[7] illustre bien

[5] Appelés « mineurs » car ils extraient des bitcoins…

[6] Dans le cas d'une fourche persistante, les mineurs retiendrons celle dont la somme des PoW est la plus forte.

[7] Pour augmenter le nombre de transactions par seconde limité aujourd'hui à 7 par seconde et pour supporter la gestion d'autres informations que les seules transactions financières comme Factom (notarisation contractuelles) ou Counterparty (extension des virements à d'autres dénominations que le BTC)

ces difficultés qui pourraient conduire à l'éclatement de la blockchain actuelle en deux blockchains distinctes donc à deux réseaux distincts.

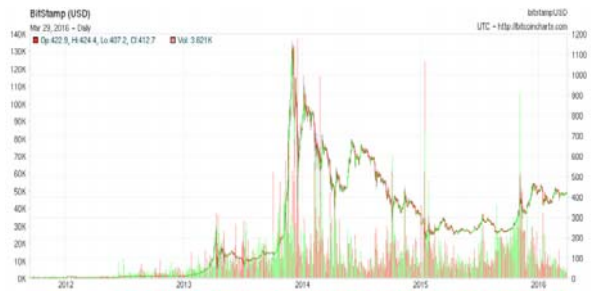
Pour optimiser leurs compromis entre gains et risques les mineurs ont formé des « pools » qui regroupent ou étendent leur moyens calculatoires. Actuellement, quatre pools minières[8] représentent près de 75% de la puissance de calcul du réseau Bitcoin. C'est un autre constat inquiétant pour la survie de l'esprit de décentralisation démocratique du réseau: la collusion des deux plus gros pools permet en théorie de prendre le contrôle de la blockchain donc du grand livre.

Protocole de consensus énergivore

En raison du très gros effort calculatoire imposé aux nœuds pour la vérification des blocs, la puissance électrique consommée en continue par l'ensemble du réseau Bitcoin est estimée aujourd'hui à environ 200 MW. A noter que cette consommation est destinée à augmenter au fil du temps car le protocole Bitcoin impose une réévaluation régulière du niveau de difficulté calculatoire pour tenir compte des améliorations[9] progressives en vitesse de traitement[10]par ajustement automatique à la puissance totale de calcul du réseau. Avec un prix moyen de 12 cents par kWh aux USA et pour un minage moyen de 150 BTC par heure[11], le coût de revient moyen d'un BTC, hors investissements, s'établit à environ 160 USD ce qui représente, en marginal, le *coût d'opportunité*, par bitcoin, pour choisir d'entrer dans le processus de minage. Tant que le cours du BTC (environ 400 USD aujourd'hui) est supérieur à ce coût, il y a une certaine logique économique à une telle consommation d'énergie. Néanmoins, il est bon de souligner que le système VISA consomme globalement cinq fois moins d'énergie pour un nombre de transactions mille fois supérieur. Cet écart donne la mesure du coût à consentir pour passer d'un système centralisé à un système distribué et la question se pose naturellement de savoir s'il est justifié.

Un statut légal mal défini

Il semble qu'il soit difficile de décider si les bitcoins sont des actifs physiques, des actifs financiers ou simplement une monnaie privée. Il n'est donc pas étonnant que leur statut juridique soit pour le moins ambiguë et variable selon les Etats. Par exemple, les bitcoins sont interdits en Russie et au Thaïlande mais sont tolérés en Europe et en France qui les considère comme une unité de compte virtuelle à caractère spéculatif. Mais puisque l'Union européenne a décidé que le bitcoin n'est pas assujetti à la TVA il semble bien qu'il y ait acquis le statut de monnaie. Aux Etats Unis, le statut du bitcoin dépend de l'Administration concernée: c'est une matière première pour l'Agence régulatrice du marché des matières premières mais c'est une monnaie pour l'IRS.



[8] AntPool, F2Pool, BTCC Pool et BitFury.
[9] Les nœuds utilisent des processeurs spécialisés ou ASIC et un haut degré de parallélisme
[10] Afin de maintenir à 10 minutes le temps moyen séparant la vérification de deux blocs consécutifs.
[11] Récompense de 25 BTC pour chaque bloque vérifié

L'absence d'un cadre juridique explicite pour les monnaies virtuelles ne peut que freiner leur force innovante mais aussi les laisser à la merci d'utilisations frauduleuses qui entretiennent leur réputation parfois un peu trop négative, au détriment d'une normalisation qui deviendra nécessaire au vu de leurs récents développements.

Limitations

On a déjà cité le faible nombre de transactions par seconde que peut réaliser le réseau Bitcoin et qui conduit les développeurs à envisager une multiplication par 8 ou 20 de la taille des blocs ce qui provoquerait une modification majeure système.

Satoshi Nakamoto a souhaité limiter intrinsèquement l'agrégat monétaire en divisant par 2 tous les 4 ans (approximativement tous les 210 000 blocs) la récompense allouée aux nœuds de minage (les mineurs). Cette création monétaire était de 50 BTC à compter de 2009, elle est aujourd'hui de 25 BTC, descendra à 12,5 BTC à la fin de l'année 2016, etc. Cette progression géométrique de raison 1/2 se terminera quand la récompense atteindra moins de 1 BTC par bloc. Elle conduit à une masse monétaire maximum d'environ 21 millions de bitcoins aux alentours de l'année 2040. Il faut noter qu'à partir de là, les mineurs devront se contenter des rétributions[12] qui leurs sont dues pour leur travail de vérification des transactions et nul ne sait aujourd'hui si l'incitation restera suffisante pour les engager à poursuivre le vrai travail de minage qui est la seule façon de conserver un consensus résistant.

[12] Le minimum « transaction fee » est fixé à 0,00001 BTC par transaction.

Risques

La forte volatilité du bitcoin le rend particulièrement vulnérable au *risque de marché*. A titre d'illustration, en partant de zéro, il a atteint 1 216 USD en novembre 2013 et il évolue actuellement (1° trimestre 2016) entre $375 et $425. Il existe aussi un réel *risque de contrepartie* en raison du peu de fiabilité ou de sérieux d'un certain nombre d'officines dédiées à l'échange des bitcoins contre les monnaies standard. Il faut aussi relever un *risque de transaction* ; en effet, ces dernières sont toujours irréversibles car le réseau Bitcoin n'offre aucune procédure de remboursement. Donc en cas d'erreur il ne faut tabler que sur la bonne volonté et la bonne foi des utilisateurs pour corriger directement entre eux les éventuels problèmes. Le caractère ouvert et distribué du réseau Bitcoin accentue les *risques opérationnels*: risque de compromission des clés privées des utilisateurs[13], risques de déni de service (DoS) sans oublier le risque global déjà mentionné de prise de contrôle du système par une attaque réunissant plus de 50% de la puissance de calcul du réseau.

Autre cryptomonnaies

Depuis l'apparition des bitcoins il s'est créé un très grand nombre d'autres monnaies virtuelles dont l'objectif est de corriger certains défauts de Bitcoin ou d'ajouter d'autres services. On en relève actuellement (mars 2016) *plusieurs centaines* (700

[13] Les clés privées permettent de signer les transactions donc de libérer les bitcoins virtuels correspondants. Leur perte est l'équivalent, pour l'utilisateur, de la perte de son portefeuille.

environ)[14]. Nous ne citerons que les vingt plus fortes capitalisations:

Nom	Symbol	Capitalisation (millions USD)
Bitcoin	BTC	6 545
Ethereum	ETH	867
Ripple	XRP	273
Litecoin	LTC	148
MaidSafeCoin	MAID	42
Dash	DASH	42
Dogecoin	DOGE	22
Monero	XMR	17
Bitshares	BTS	15
Factom	FCT	15
NEM	XEM	13
Emercoin	EMC	12
Stellar	XLM	11
Peercoin	PPC	11
FedoraCoin	TIPS	9
Nxt	NXT	8
Bytecoin	BCN	8
Namecoin	NMC	7
Synereo	AMP	6
Agora Tokens	AGRS	6

Certaines de ces cryptomonnaies se distinguent du modèle initial Bitcoin principalement par leurs capacités à gérer, en plus d'une monnaie virtuelle, d'autres types d'actifs en utilisant le même principe de tiers de confiance distribué. Elles peuvent aussi proposer des constructions plus rapides des blocs en vue d'accélérer les transactions ou un plus grand nombre de transactions par unité de temps. Certaines d'entre elles, par exemple Peercoin ou Nxt, utilisent un principe de consensus différent du « Proof of Work » de Bitcoin: la « preuve de part » ou « Proof of Stake » (PoS) qui est liée à la quantité de monnaie virtuelle (la part) détenue par chacun des utilisateurs habilités à participer au vote majoritaire du consensus décidant de la validité d'un bloc. En effet, si le nombre de votes est proportionnel au nombre d'unités de monnaie virtuelle détenue, il est clair qu'il n'est possible de prendre le contrôle du réseau que si l'on détient soi-même plus de 50% de la capitalisation ce qui paraît d'une part très difficile et d'autre part assez inutile puisque cela revient alors à s'attaquer soi-même. La mise en œuvre de cette nouvelle preuve de consensus a surtout été motivée pour éviter d'aboutir au même problème de consommation énergétique que celle provoquée par la preuve de travail de Bitcoin. Certains mettent en avant une faiblesse possible du PoS, appelée le « nothing-at-stake », arguant que si la blockchain présente une fourche, les utilisateurs participants au vote n'auront rien à perdre et tout à gagner en votant successivement pour les deux chaînes ce qui entraine immédiatement des possibilités de double dépenses, invalidant ainsi complètement le système. Une parade retenue par certaines cryptomonnaies consiste en un mélange de PoW du type Bitcoin et de PoS: le PoW est utilisé périodiquement pour valider la bonne blockchain; ainsi le travail énergiquement coûteux de minage se trouve un peu dilué.

[14] Voir par exemple http://coinmarketcap.com/all/views/all/

Cryptomonnaies 2.0

Tout système de monnaie virtuelle peut être vu comme la résultante des éléments distincts suivants:

- Un token (par exemple le bitcoin)
- Des règles de transactions Peer-to-Peer de ces tokens, gérant des adresses, veillant aux signatures cryptologiques[15] des échanges, à la création des clés, à la diffusion des échanges sur le réseau, aux balances des comptes s'il y a lieu, etc.
- Un réseau, en général Internet, assorti des protocoles particuliers au système, notamment entre nœuds et entre nœuds et utilisateurs,
- Un grand livre infalsifiable et « indestructible » sous la forme d'une base de données particulière répliquée dans tous les nœuds, la *Blockchain*,
- Un processus de *consensus* décentralisé ayant pour objet de créer une confiance ou un accord global entre des parties ne se faisant pas confiance a priori, qui peuvent être anonymes et non nécessairement présentes au départ du processus.

En retenant tout ou partie de ces fonctions ou en modifiant chacune d'elle on peut obtenir une très grande variété de systèmes qui seront plus ou moins performants ou plus ou moins adaptés à tel ou tel service: des « trust machine ». C'est ce qu'il n'a pas manqué de se produire dans le cadre de ce qui est appelé maintenant « cryptocurrencies 2.0 ».

Nous avons déjà constaté qu'il existe plusieurs types de méthodes d'établissement d'un consensus « distribué »: les preuves de travail (PoW) et les preuves de parts (PoS), chacune d'elles possédant des variantes, par exemple le « proof-of-burn »[16]. Bien d'autres formes de preuves de travail sont concevables[17] faisant toujours appel à des limitations de ressources.

Pour ce qui concerne les services, on a pu constater le développement de centaines de monnaies virtuelles comme alternatives à Bitcoin. Mais les mêmes principes peuvent être appliqués à tout actif « numérisé » profitant ainsi de la confiance décentralisée et de la solidité de la blockchain[18]. Une première voie consiste à surajouter à la cryptomonnaie l'actif en question pour en faire une metadata parfois appelée « colored coin » dans la littérature. Une autre voie est de réaliser des réseaux spécifiques ou au contraire complètement adaptables au service recherché (c'est le cas par exemple d'Ethereum). On peut également introduire la notion de « *Blockchain privée*[19] » où c'est la fonction de grand livre fiable et infalsifiable qui prime entre partenaires qui se font confiance; de fait, le processus de consensus distribué n'est plus nécessaire tandis que la blockchain garanti une synchronisation fiable entre les différents acteurs (des réseaux bancaires s'intéressent au sujet[20]). Il existe également une large gamme d'applications

[15] Par paire de clés privée/publique sur courbes elliptiques (ECDSA, standard secp256k1)

[16] Consiste à rendre inutilisable un certain nombre de ses propres tokens comme preuve de travail

[17] Cuckoo Cycle: a memory bound graph-theoretic proof-of-work, John Tromp, December 31, 2014

[18] Great Chain of Numbers a guide to smart contracts, smart property and trustless asset management, Tim Swanson

[19] MultiChain Private Blockchain – White paper, Dr Gideon Greenspan

[20] De la finance à l'IoT, la révolution blockchain est en marche, Aude Fredouelle

réunies sous le vocable de « smart contracts » que l'on peut définir comme des outils pour automatiser et « graver dans le marbre » des interactions contractuelles comme par exemple des contrats d'assurance ou des paiements échelonnés; l'existence de la crypto-monnaie dans le système permet d'envisager le déclenchement automatique des règlements financiers entre des parties liées contractuellement sans l'intervention de tiers extérieurs.

Quelques références pour aller plus loin

Fonctionnement détaillé du réseau Bitcoin et ses fonctions cryptologiques:

Mastering Bitcoin, Andreas M. Antonopoulos, oreilly.com

Bitcoin Book, Pierre Noizat, (2012)

Understanding Bitcoin, Pedro Franco, (2015), Wiley
A Treatise on Altcoins, Andrew Poelstra
Aspects économiques:

Bitcoin: Economics,Technology, and Governance, Rainer Böhme, Nicolas Christin, Tyler Moore, Benjamin Edelman
The Economics of Bitcoin Mining, Josua A. Kroll, Ian C. Davey, Edward W. Felten
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, Andrew Miller
The great chain of being sure about things, The Economist, Oct 31st 2015
Problèmes de consensus:

Impossibility of Distributed Consensus with One Faulty Process, Michael J. Fischer
Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin, Andrew Miller, Joseph J. La Viola
The Sybil Attack, John R. Douceur
The Byzantine Generals Problem, Leslie Lamport, Robert Shostak, Marshall Pease
Distributed Consensus from proof of Stake is Impossible, Andrew Poelstra
On stake and Consensus, Andrew Poelstra
Majority is not Enough: Bitcoin Mining is Vulnerable, Ittay Eyal, Emin Gün Sirer

LES TAUX BAS SONT-ILS UN PIEGE MORTEL ?

(suite)

Traditionnellement, l'emprunteur compte sur l'inflation pour éroder le poids de ses remboursements et de ses intérêts. Cela est le cas de l'État qui en période de croissance forte et d'inflation moyenne ou forte voit ses rentrées augmenter et la charge de sa dette réduite par l'augmentation des prix.

Dans le triple souci de permettre aux banques de faire face à leurs nouvelles obligations réglementaires (Bâle 3 en particulier), d'éviter les faillites des États et de relancer le crédit, les banques centrales ont pris différentes mesures dites non conventionnelles dont le but est d'émettre de la liquidité. Certes, à la suite de ces mesures, en Europe la demande et les investissements se sont accrus entraînant une baisse du chômage. Mais ceci n'a été possible que parce que des mesures d'assouplissement des conditions du travail ont été prises soit il y a quelques temps (Allemagne) soit plus récemment (Espagne, Royaume-Uni, Italie,). La France ne bénéficie pas de cette reprise car les tentatives du gouvernement ont connu les blocages que l'on sait.

Cet afflux de liquidité a fait baisser les taux, les rendant négatifs D'autre part le taux directeur de la banque centrale (– 0,4%) pousse les institutions financières à gérer leur trésorerie à court terme en se procurant des emprunts d'État à court terme moins pénalisant que les dépôts à la Banque négatifs selon les maturités les rendements de ces mêmes emprunts.

Les avantages ayant été définis, quels sont les inconvénients des taux bas voire négatifs ?

En ce qui concerne la Banque de Financement et d'Investissement (BFI): les activités de taux sont en recul dans la mesure où les marges sont compressées. Ceci a entraîné une réduction de l'activité taux des BFI avec pour corollaire toute une série de licenciements et ce n'est pas fini : on prévoit encore 10% pour les front-offices et 15% pour les back-offices[21].

En ce qui concerne les compagnies d'assurance-vie le problème devient de plus en plus aigu. En effet, les contrats d'assurance en euros sont établis sur un engagement minimum de rendement (indépendamment de la participation aux bénéfices). Ce niveau de rendement est très supérieur à ce que le marché peut fournir en matière de placement (et compte tenu des règles prudentielles propres aux compagnies d'assurance comme Solvabilité 2). Jusqu'à présent les compagnies peuvent continuer à verser des rendements correspondants à leurs engagement, dans la mesure où la baisse des taux à permis de réaliser des plus values sur les obligations qui étaient détenues (la valeur de marché d'une obligation variant de façon inverse au mouvement des taux) et donc de disposer de provisions pour faire face aux engagements. La question se pose de savoir combien de temps elles pourront tenir. En France une bonne partie des assurés épargnent pour leur

[21] Les Échos 15 Mars 2016.

retraite. Avec des taux d'intérêt négatifs l'épargne ne rapporte plus rien, bien au contraire elle fait perdre du pouvoir d'achat futur. Ainsi les taux d'intérêts bas ou négatifs posent le problème du financement des retraites pour les futurs retraités. La question est de savoir si ces derniers accepteront de se faire tondre. Bien sûr, une solution existe consistant à basculer les fonds d'assurances vers des investissements plus rentables sous la forme d'unités de compte, mais cela implique une prise de risque minimum que les assurés ne sont pas forcement prêts à prendre.

L'objectif de la BCE était de pousser les agents économiques (et en particulier les ménages mais aussi les entreprises) à consommer et à investir plus, mais le climat fait qu'aux dépenses de consommation les agents économiques préfèrent l'épargne. L'augmentation de celle-ci résultant de la constitution d'encaisses de précaution, conséquence des inquiétudes sur l'avenir.

Un autre effet, plus technique, mais avec des conséquences importantes, consiste à la difficulté de procéder à des calculs d'actualisation avec des taux négatifs ou très bas. L'actualisation permet de ramener les flux futurs perçus à partir d'un investissement à une valeur actuelle. C'est la base d'évaluation (pricing) d'un investissement quelque-il soit. En effet, un actif s'évalue à partir de la somme des flux perçus dans le futur, une fois ces derniers actualisés. Si le taux d'actualisation est très bas la valeur future est proche de la valeur actuelle et le risque est alors sous-évalué. Certes, avec un taux d'inflation bas, la valeur actuelle et la valeur future sont proches, mais ce calcul ne prend pas en compte les variations futures (qui ont de fortes chances de se produire).

CONCLUSIONS

Les taux d'intérêt bas recèlent potentiellement des risques importants et ce d'autant plus qu'ils sont relativement inconnus. En général les taux d'intérêt ont tendance à revenir vers leur moyenne historique, que l'on peut évaluer entre 3 et 5% selon les époques et les pays ou encore vers la moyenne du taux de croissance d'une économie. Si cela n'est pas le cas on rentre dans un territoire totalement inconnu. La question est de savoir si les politiques de taux bas qui sont menées sont d'ordre conjoncturel ou bien compte tenu des circonstances (par exemple surendettement des États) ils ont vocation à durer longtemps provoquant ainsi ce que Keynes appelait « l'euthanasie des rentiers », c'est-à-dire la ruine des épargnants, et cela pour faire face à l'impéritie des gouvernements.

Ceci étant dit, la vraie question est de savoir comment on sortira de cette situation. IL faut d'abord ne pas verser dans le catastrophisme. Si on n'a pas connu des taux nominaux négatifs par le passé, on a déjà connu des taux réels négatifs dans les années 70, l'inflation étant supérieure à la rémunération des placements à taux fixes. Certes psychologiquement l'effet n'est pas le même et une illusion monétaire existe alors.

La solution repose comme d'habitude sur une augmentation des taux de croissance des économies dites développées. Mais cette croissance ne pourra se faire qu'avec une prise de risque plus élevée. L'histoire nous

donne d'ailleurs une bonne leçon : le monde occidental est sorti de l'atonie économique de la fin du moyen âge par la prise de risque en matière d'exploration et de développement du commerce lointain. Mais ce développement a surtout été possible dans les états où le gouvernement comme on le dit maintenant « business friendly » : en France, les foires de Champagne n'existèrent que grâce à la politique libérale des comtes de Champagne, idem pour les Pays bas et bien d'autres exemples encore. Les Espagnols ne surent profiter à plein des découvertes des terres américaines car la rapacité du gouvernement et le carcan législatif empêchèrent le pays de faire fructifier les richesses, laissant aux génois l'exploitation financière de la manne américaine.[22]

Ainsi nous ne sortirons par le haut de cette situation que si les États comprennent que la croissance est le fait d'entrepreneurs aventuriers et que ces mêmes États ne disposent d'aucun moyen de la relancer sauf à réduire les dépenses de l'État et augmenter sa productivité.. Ceci implique, en particulier dans notre pays, que L'État se mêle moins de la vie économique et qu'au contraire il s'emploie à ôter les carcans qui bloquent toutes les initiatives individuelles. Nous avons malheureusement actuellement l'expérience de la gestion de l'État dans les sociétés publiques : EDF, Area, SNCF entre autres. Cela implique naturellement moins d'assistanat, moins de taxation du capital, moins de dépenses publiques non productives et beaucoup moins de serviteurs de l'État qui dans notre système sont assimilables à des rentiers[23] qui on le veuille ou non détournent la valeur produite. Ce n'est pas un jugement sur les hommes mais sur des structures désormais totalement inadaptées au monde moderne.

[22] Lire à ce sujet le magnifique ouvrage de Philippe Chalmain et Alessandro Giraudo « Au temps des comptoirs », François Bourrin Editeur, paris 2010

[23] Le rentier est celui qui bénéficie de revenus provenant d'une situation et sans lien avec son activité. L'emploi à vie est de ce fait une rente quand il n'est pas lié aux résultats. Les gouvernements ont bien compris cela, soit en supprimant l'emploi à vie, soit en liant la rémunération au mérite.

Stratégies & Information

« Seul le vide pénètre là où il n'y a pas de faille » Lao-Tseu

Stratégies et Informations

Lettre d'analyse économique et de cognitique financière Relative à l'évolution des marchés

Éditée par SIGRE PRESSE
45,Boulevard de Courcelles
75008-Paris
Tel :003345665058
Fax :OO3342277199

Directeur de la Publication : Andrea Brignone

Rédaction :
Andrea Brignone
Laure Brignone
Anne de Canecaude
(Los Angeles)
Herbert Groscot
Edouard Hostin
Joël Lebidois
Yuri Rudakovsky
(Moscou)
Et
Janus

Lettre publiée sous forme électronique

ISSN-1254-8103
Prix au numéro : 20 €
Abonnement :12 numéros 200€

Editorial

Dans ce numéro, vous trouverez un article de Joël Lebidois, grand spécialiste de la cryptographie et aussi de la finance. Il est entre autre l'auteur de *Finances pour Ingénieur* , Maxima , Paris 2013. Cet article fait un point très clair sur les crypto-monnaies et les blockchains , grand sujet d'intérêt dans le monde bancaire. Il fait aussi partie de ce groupe de réflexion que nous avons crée sur les méthodes de la finance quantitative et de la gestion des risques avec Herbert Groscot, mathématicien et actuaire. Finalement vous trouverez régulièrement des indicateurs de chargements maritimes auxquels nous avons fait allusion dans notre numéro de février :

Baltic index dry : 400 au 22/04 plus bas février 290. Cet indice ne fait que monter montrant une croissance de la demande de fret pour les matlères premières, signe d'une reprise des économies émergentes et des autres. HARPER Index (conteneurs) : 358 au 16/04/au minimum, aucune reprise, sur la demande de fret pour les produits manufacturés. Baltic index tanker : 538 pour le Clean Index, petite reprise pour les chargements de dérivés du pétrole. 790 pour le dirty (le minimum était autour de 700 en mars, légère reprise mais qui peut s'expliquer aussi par la nécessité d'utiliser les tankers comme unités de stockage.

PROCHAINS SEMINAIRES D'ANDREA BRIGNONE

INITIATION AUX PRODUITS DERIVES

27 MAI

GESTION DES RISQUES DE POSITION ET PROTECTIONS CONTRE LE RISQUE DE TAUX

31 MAI-1ER JUIN

TECHNIQUES DE LA TITRISATION

13-14 jUIN

PRODUITS DE TAUX FERMES ET DÉRIVÉS

22,23 et 24 jUIN