



Blockchain et Enjeux de supervision

France Stratégie 4 mai 2017

Grands principes de supervision

- ❑ **Protection des consommateurs/investisseurs**
- ❑ **Sécurité des transactions**
- ❑ **Lutte anti-blanchiment**
- ❑ **Stabilité financière**

Protection des consommateurs et sécurité des transactions

- ❑ **Communication Loyale et Transparente**
- ❑ **Sécurité juridique**
- ❑ **Protection des données**
- ❑ **Confidentialité**
- ❑ **Droit à l'oubli**
- ❑ **Sécurité technique: cyber-sécurité, risques opérationnels**

Lutte anti-blanchiment, stabilité financière

□ LCBFT

- A distance: facteur de risque élevé (GAFI)
 - Connaissance des clients
 - Incompatibilité pseudonymisation
- Traçabilité des flux financiers
- Shadow banking/insurance – économie parallèle

□ Stabilité financière

- Contagion en cas de défaut d'activité systémique
- Résolution des activités

Intéropérabilité des systèmes

Interactions avec Blockchain

- Selon les typologies de Blockchains
 - Publique
 - Privée
 - Publique permissionnée , Consortium
- Selon les cas d'usages envisagés
 - Optimisation de process internes d'acteurs régulés
 - Réduction du maillage d'intermédiaires dans infrastructures financières
 - Activité financière BtoC directement régulée

Blockchain et désintermédiation

- Cas atypique de Bitcoin
 - Optique libertarienne
 - Délibérément sans autorité centrale
 - Mais
 - Concentration des mineurs
 - Concentration des codeurs
- Discours inspiré de cette philosophie...
- ...Mais porté par des INTERMEDIAIRES !
- Évolution de leur rôle mais adoptent position centrale dans les projets

Utilisation de Bitcoin ?

- Bitcoin pas une Monnaie électronique-> monnaie virtuelle
 - -> établissements agréés dès lors qu'Euro<->Bitcoin
 - -> soumission LCBFT des plateformes Bitcoin (7Bis L561-2 CMF)
- Pas d'utilisation pour activités régulées (ex: DVP)
- S'applique aux autres cas de monnaies virtuelles
Générateur de forts risques:
 - -> Non régulé et n'offrant aucune garantie de sécurité, de convertibilité ni de valeur
 - -> Conception qui alimente la spéculation
 - -> Anonymat qui favorise le contournement des règles LCBFT
 - -> Pour en savoir plus : https://publications.banque-france.fr/sites/default/files/medias/documents/focus-10_2013-12-05_fr.pdf

Blockchain Bitcoin & Trust Protocol

- Aspects intéressants de BB pour les acteurs:
 - Sa durée de vie
 - Sa taille (dont nombre de nœuds de réplication)
 - Sa transparence
 - Son universalité (accès entièrement public non contrôlé)
 - La présence d'une forme de « monnaie »
 - Sa gouvernance décentralisée / indépendante
- Mais limitations pour les Autorités:
 - Durée de vie : preuve de qualité ou intérêt d'acteurs
 - Taille: localisation des registres (GDPR)
 - Universalité: LCBFT
 - Pas une monnaie à cour légal (pas de pouvoir libératoire)
 - Transparence: incompatible avec secret des affaires
 - Gouvernance: pas de responsable identifié, mais en sus incertitude sur réelle indépendance
- Malgré aspects intéressants, impossible d'en promouvoir l'utilisation directe comme indirecte (fonctionnements sidechains).

Autres Blockchains Publiques

- Intérêt d'une blockchain publique est fortement lié à sa taille:
 - Nombre de nœuds facteur de sécurité
 - Existence longue -> intérêt de participants à son maintien
 - Plus de « mineurs » -> plus de travail « incorporé » dans le mécanisme de confiance plus difficile à « craquer »
- Intérêt = Autres fonctionnalités (ex. Smartcontracts)
- Aspects rédhibitoires de Bitcoin restent présents
- Question d'utilisation de la technologie sous-jacente dans un cadre régulation-compatible.

Blockchains privées

- Utilisation de certains principes sous-jacents aux blockchains publiques
- Dans un environnement privé:
 - Gouvernance centralisée (code, accès etc.)
 - Nœuds physique de réplication des registres contrôlés par Autorité centrale
 - Protocole de consensus défini par autorité centrale
- Outils technologiques alternatifs de gestion de l'information :
 - Sécurité accrue par répartition sur plusieurs nœuds
 - Registre unique partagé d'enregistrement d'informations en temps réel

Blockchains privées

- Peuvent a priori entrer dans le cadre « classique »
- Avec des points d'attention particuliers
 - Protection des données (notamment selon emplacement physique de réplication + problème droit à l'oubli)
 - Risque opérationnel / cybersécurité (moins résistant qu'une Blockchain publique de ce point de vue)
- Et incontournables (le terme « Blockchain » n'en dispense pas)
 - Protection des consommateurs / investisseurs (conseil, validité du contrat, de sa signature...)
 - LCBFT
 - Sécurité des transactions / engagements
- Notamment l'intégration de solutions de paiement dans les modèles peut poser problème

Blockchains publiques permissionnées

- Les Blockchains privées perdent certaines caractéristiques intéressantes des publiques:
 - Réduction du nombre de nœuds donc de sécurité
 - Pas de renforcement de confiance en environnement décentralisé
 - Utilisations limitées en BtoC
- D'où l'utilisation de solutions hybrides
 - Intégrant en général une certaine centralisation de gouvernance (dont du code et des droits d'accès)
 - Avec des protocoles de consensus moins coûteux que PoW mais comportant un renfort de confiance minimal
 - Avec un nombre de nœuds de réplication assez important
 - Avec un masquage total ou partiel des transactions
- Dont l'acceptabilité dépendra de ce qui est précisément adapté par rapport aux exigences du cas d'usage

Blockchains publiques permissionnées

- Points d'attentions:
 - Utilisation de « sidechains »
 - Mode de gouvernance : qui contrôle le code, les accès, le protocole de consensus ?
 - Niveau de sécurité
 - Nœuds de répliquations
 - Type de protocole
 - Questions juridiques (droit du contrat, droit de propriété)
 - Valeur de ce qui y est inscrit
 - Utilisation de smartcontracts
 - Signature électronique
 - Conformité formelle aux textes

Blockchains publiques permissionnées

- Points d'attentions:
 - Questions pratiques
 - Interopérabilité entre différentes solutions
 - Modalités d'exit en cas d'arrêt
 - Articulation LCBFT/Performance/Transparence
 - Connexion avec autres services financiers (paiement)
 - Modalités de supervision / implication du superviseur (responsabilités associées)
 - Articulation avec GDPR (responsable de traitement)
 - Probables cas d'usages combinant acceptabilité du superviseur/régulateur et intérêt économique
 - -> à confirmer concrètement

SandBox et Blockchain ?

- Pour quelle Blockchain ?
 - Si publique type Ethereum ou Bitcoin, peu utile car difficile d'imaginer aller au-delà
 - Si privée ou publique permissionnée:
 - Attention à quelles réglementations concernées
 - Quel périmètre d'activités régulées ?
 - Nota: SandBox ne répond pas aux questions de scalabilité et risques lié à de l'usage en mode « systémique »
 - Or plusieurs projets affectent infrastructures systémiques (paiement, marchés)
 - Et sujets hors champ financier (GDPR) ou trop sensibles (LCBFT)
- Préférence d'approche française :
 - Champ d'expérimentation – à faible enjeu – doté d'une réglementation effective
 - Extensions selon apprentissage (de tous) sur ces cas concrets

Annexe

- Consultation DGT : ordonnance pour l'utilisation de Blockchain pour titres non cotés.
- Délai réponse au 19 mai
- http://www.tresor.economie.gouv.fr/16101_consultation-publique-ordonnance-blockchain-applicable-a-certains-titres-financiers