Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Conférence de presse annuelle du 27 mars 2018

Mark Branson, Directeur de la FINMA

Technologie et branche financière : opportunités et risques

Mesdames, Messieurs,

Je consacrerai mon discours d'aujourd'hui aux rapports existant actuellement entre technologie et branche financière pour en détailler à la fois les opportunités et les risques. Les concepts-clés dans ce domaine sont bien connus : *blockchain*, ICO, *big data*, cyberrisques, etc. Mais que cachent ces expressions qui font la une des journaux ?

Au regard des taux d'intérêt bas, de la rentabilité en berne et des nouveaux comportements des clients, l'innovation peut être un sujet important, voire crucial, pour l'industrie financière.

L'innovation ne peut pas être prescrite au niveau étatique, mais constitue une tâche incombant avant tout à l'industrie elle-même. En tant qu'autorité de surveillance, nous voulons toutefois nous assurer que le dispositif réglementaire permette d'innover. Ce n'est pas là une politique structurelle déguisée ; il s'agit de réduire les obstacles à l'entrée sur le marché afin de garantir une saine concurrence.

Etre favorable à l'innovation n'implique toutefois pas de faire preuve de naïveté. La numérisation et l'innovation dans le domaine financier conduisent à de nouveaux risques ou permettent le retour d'anciens dangers drapés de nouveaux oripeaux. C'est notre tâche, en tant qu'autorité de surveillance, de connaître ces risques, de les surveiller et de les limiter si besoin est. Je pense ici notamment aux risques de blanchiment d'argent via le système de la *blockchain*, aux risques de perte pour les personnes investissant dans des ICO ou encore à l'importance des cyberrisques.

La promesse des Fintech

Mais laissez-moi tout d'abord passer en revue les opportunités que présentent les Fintech. Un grand nombre de nouveaux produits et de nouvelles applications font leur apparition sur le marché. Des projets se réalisent via des schémas de financement participatif, des fonds sont transmis à partir d'un simple téléphone portable, de nouvelles couches de la population des pays émergeants ont accès à des prestations financières et des « robots » prennent des décisions de placement.

Laupenstrasse 27
3003 Berne
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

Nous reconnaissons le potentiel important des Fintech et de la *blockchain* pour la place financière. Nous y voyons aussi un rôle à jouer pour nous en tant qu'autorité de surveillance : nous voulons permettre l'innovation. Nous l'avons déjà démontré à plusieurs reprises. Nous donnons par exemple à notre réglementation une forme résolument neutre à l'égard de la technologie, sans faire de distinction entre canaux numériques et analogiques. La FINMA a en outre lancé l'idée d'un « bac à sable » et d'une licence spécifique aux Fintech. Nous avons aussi donné, dans la mesure du possible, des informations pratiques aux personnes exploitant des ICO.

Notre but est que les innovateurs apportent une saine concurrence sans que l'intégrité de la place financière ne s'en trouve menacée. Si nous sommes pro-innovation, nous n'en restons pas moins anti-criminalité financière.

La *blockchain* : mode passagère ou réel moteur pour l'innovation ?

La *blockchain* est une technologie intéressante. L'on peut par exemple s'imaginer qu'une partie de l'actuelle infrastructure des marchés financiers devienne un jour obsolète, réalisant ainsi la prophétie de Bill Gates lorsqu'il disait en 1994 : *« Banking is necessary, banks are not »*.

Cette technologie est déjà très utilisée dans le contexte des cryptomonnaies et des ICO. D'une méthode peu connue de rassembler des fonds, les ICO sont devenues, en peu de temps, de véritables « aimants financiers », capables d'attirer plus de six milliards de dollars au niveau mondial sur la seule année 2017. Sur les six plus grands ICO, quatre ont eu lieu en Suisse. Le pays est ainsi devenu un pôle important en la matière. Il n'est donc pas étonnant que la FINMA reçoive des dizaines de demandes. Cela nous a poussés à expliquer de manière transparente, dans un guide pratique, la manière dont nous y répondons en nous fondant sur les lois existantes.

Les premières réactions à cette démarche ont été positives, les prestataires sérieux ayant salué cette initiative. Ils savent que l'absence généralisée de règles restera toujours une utopie.

Dans tout l'enthousiasme qui gagne parfois le marché, il ne faudrait pas oublier que les cryptomonnaies comportent des risques. Une approche absolument libertaire nous semble peu judicieuse. Les variations de valeur sont extrêmes. De plus, les risques ne sont souvent pas présentés de manière transparente aux clients des ICO. Fréquemment, les projets n'ont été lancés que récemment et les informations disponibles à leur sujet sont rudimentaires. Le risque de défaut, comme pour d'autres investissements dans des start-ups, ne sont pas négligeables. C'est aussi un terreau fertile pour des activités de blanchiment d'argent. De nombreux prestataires de cryptomonnaies mettent justement en avant leur caractère opaque et anonyme. Enfin, les plates-formes de négociation de cryptomonnaies ont été les cibles de hackers, ces attaques engendrant des dommages de centaines de millions de dollars. D'où notre approche simple : les ICO de jetons ou de cryptomonnaies sont soumis à la loi sur le blanchiment d'argent, alors que les ICO qui proposent des possibilités d'investissement doivent être traités comme des opérations sur valeurs mobilières

Cyberrisques : les attentes de la FINMA

Les attaques de hackers mentionnées ci-dessus me donnent l'occasion d'évoquer le thème des cyberrisques pour les établissements financiers. Ceux-ci sont une cible de choix pour les hackers et

autres formes de cyberattaques. Les dernières statistiques de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI le montrent : deux tiers des attaques sur des infrastructures d'importance critique concernent le secteur financier.

Le risque de telles attaques augmente avec la numérisation. Les cyberattaques sont devenues le principal risque opérationnel pour le système financier. Nous devons tous – tant le secteur privé que les autorités – prendre ce thème très au sérieux. En principe, nous constatons que nos assujettis se montrent très sensibles à cette problématique et qu'ils semblent bien préparés. De nombreuses attaques sont déjouées chaque jour. Par exemple, en relation avec le maliciel « Retefe », jusqu'à 100 attaques sur des solutions d'e-banking ont été quotidiennement constatées en Suisse.

Cependant, même le meilleur système de défense a ses points faibles. Des hackers ont ainsi pu accéder au système international de paiement Swift après avoir pénétré le système de la banque centrale du Bangladesh. En Suisse, de grandes quantités de données clientèle ont récemment été volées à une caisse-maladie.

Quelles sont les attentes de la FINMA concernant ces risques ? Il est primordial que les établissements financiers connaissent leur propre vulnérabilité. Les tests de pénétration sont des instruments importants à cet égard. La capacité de réaction est également importante en cas de cyberattaques. Face à un tel événement, l'activité doit reprendre aussi vite que possible. Chaque établissement doit établir et entretenir pour son activité un dispositif de crise qui fonctionne.

Les risques dépassent toutefois largement les simples vols de données ou d'argent. Des attaques ciblées, provenant parfois même d'organisations étatiques, semi-étatiques ou terroristes, pourraient prendre une ampleur systémique. Si les établissements financiers suisses semblent correctement armés en comparaison internationale, nous constatons que la Suisse en tant que pays est moins active que d'autres nations pour protéger le système dans son ensemble. Ainsi, certains pays disposant aussi d'une place financière importante bénéficient par exemple d'un service central compétent en matière de cybersécurité ou organisent des tests de pénétration à l'échelle du système. Un monitorage du système dans son ensemble avec des processus en proportion devrait être mis en œuvre en Suisse – et la FINMA se déclare prête à y jouer un rôle important. Nous avons recruté de manière ciblée des spécialistes dans ce domaine et nous ne reculerons pas devant d'autres investissements dans cette direction.

Le comité consultatif « Avenir de la place financière », sous la direction du professeur Brunetti, a élaboré trois importantes recommandations pour la cybersécurité de la place financière helvétique. Celles-ci ont suscité peu d'intérêt du public. A tort.

Tout d'abord, l'accès à la centrale MELANI devrait être élargi, notamment en direction des petits établissements financiers suisses. Ensuite, il conviendrait d'institutionnaliser et de renforcer la collaboration entre les experts de la branche financière et les autorités. Il y a peu de domaines où les intérêts des sociétés privées rejoignent autant ceux de la surveillance que dans la lutte contre les cyberrisques. Enfin, il faudrait mettre au point et tester un dispositif de sécurité en cas de cybercrise propre au secteur financier.

La FINMA salue expressément les recommandations du comité consultatif « Avenir de la place financière » et entend y apporter son soutien. Ensemble, nous y arriverons mieux qu'en faisant cavalier seul. La Suisse fait déjà des efforts dans ce sens, mais d'autres pays en font beaucoup plus.

Les effets de concentration liés aux externalisations

Un phénomène vient renforcer la menace de cyberattaques : l'externalisation croissante de processus d'exploitation ou de l'infrastructure informatique.

Une grande majorité des banques suisses ont externalisé des divisions de première importance. Parfois, elles externalisent l'ensemble de leurs processus de *backoffice*. Cette évolution place aussi la surveillance face à de nouveaux défis.

Nous observons en particulier une forte concentration sur certains prestataires en Suisse. Beaucoup de banques leur ont confié leurs prestations de service. Nous leur appliquons donc les mêmes critères que pour les établissements financiers eux-mêmes. Depuis 2016, nous disposons des bases légales nous permettant d'aller nous-mêmes sur place pour contrôler les partenaires des établissements financiers. Nous avons déjà effectué de tels contrôles sur place auprès de prestataires de ce genre et nous poursuivrons avec résolution dans cette direction.

Saisir les opportunités, identifier les risques

Les Fintech ont un grand potentiel. En tant qu'autorité de surveillance, nous ferons tout notre possible pour permettre au secteur financier de se montrer innovant. Ce sera au marché et aux clients, et non aux conditions-cadres réglementaires, de décider si les applications de ces technologies tiennent leurs promesses. C'est là notre principe.

Le monde des cryptomonnaies voit défiler aussi bien des innovateurs que des profiteurs, des arbitragistes et des escrocs. Notre tâche est, avec nos autorités partenaires, de donner aux innovateurs sérieux la possibilité de réussir, d'empêcher les arbitrages et de placer les escrocs là où ils méritent d'être. Tant les opportunités que les risques que recèlent les nouvelles technologies requièrent toute notre attention et tout notre engagement.

Je vous remercie pour votre attention.