



Royaume-Uni

NOUVEAUX MOYENS DE PAIEMENT, Outils ET ENJEUX DE STRATEGIE NATIONALE

BERRAMDANE Enzo, BRUNEAU Sarah, BUCHMÜLLER Thérèse, DARRAZ Marwan, DAVID Bénédicte, LUGO Nicole, MODOL Robinson, Julien VACHEL

Table des matières

INTRODUCTION.....	3
PARTIE 1 : Etat des lieux des moyens de paiement au Royaume-Uni.....	5
Chapitre 1 : Acteurs et fonctionnement du système de paiement britannique.....	5
Les banques et les opérateurs au cœur du système des moyens de paiement.....	5
Les institutions financières au Royaume-Uni	6
Chapitre 2 : La diversification des nouveaux moyens de paiement : l'entrée en force des Gafa et des Fintechs.....	10
État des lieux des modes paiement en 2017.....	10
Les acteurs des nouveaux modes de paiement et l'influence américaine.....	11
PARTIE 2 : La mise en œuvre d'une stratégie nationale limitée	14
Chapitre 1 : Un système à la vulnérabilité grandissante	14
Des failles renforcées par l'élargissement de la chaîne de transmission des données	14
Le Royaume-Uni : mauvais élève de la cybersécurité.....	16
Chapitre 2 : Face à une stratégie de libéralisation des données, un contrôle suffisant des données ?	18
La Nouvelle Architecture des paiements : une stratégie nationale de modernisation des systèmes de paiement et de libéralisation du partage de données.....	18
L'Open Banking : la mainmise des acteurs non-bancaires sur les données des transactions bancaires du Royaume-Uni.....	20
Les cryptomonnaies : une technologie de rupture	24
Encadrement légal de la donnée au Royaume-Uni	28
Chapitre 3 : Des données personnelles en otage : le danger des datasbrokers et l'influence américaine	31
Databroker : le middle-man de la data.....	31
L' <i>USA dependence</i> au cœur de la captation des données britanniques.....	32
Brexit : La perspective d'une influence accrue des Etats-Unis sur le contrôle des données britanniques ?	35
CONCLUSION.....	37
GLOSSAIRE	38
BIBLIOGRAPHIE	40
ANNEXES.....	50

INTRODUCTION

Le domaine bancaire au Royaume-Uni, plus que pour tout autre pays, a joué un rôle central dans sa stratégie d'accroissement de puissance. Il a été, depuis l'époque victorienne- ère marquant l'apogée de l'empire britannique- un des fondements de sa puissance économique et militaire.

D'abord portée par le secteur industriel à l'aube du XVIII siècle, ce dernier connaît des déconvenues dans les années 1850. Ces difficultés conduisent alors l'empire britannique à développer le secteur financier. La montée en puissance du quartier de la City, à Londres, devient la marque emblématique de ce succès. La City devient un véritable outil de puissance pour l'Empire. La capacité phénoménale d'emprunt du Royaume-Uni fut, par exemple, une des conditions de la victoire anglaise sur la France en 1759 (un tiers de l'effort de guerre fut financé par des prêts). À cette époque, l'empire britannique dynamise le secteur bancaire par l'innovation et la création de normes, qui vont peu à peu s'imposer au reste du monde. Le rôle prépondérant de la City est ainsi soutenu par la livre sterling, basée sur le système monétaire de l'étalon or, qui devient la monnaie d'échange internationale. La solidité de la livre sterling permet à la City de garantir des financements colossaux à ses clients, ce qui la transforme en une plaque tournante de l'économie mondiale. La City innove aussi dans les moyens de paiement. À partir des années 1870, elle remplace, par exemple, les lettres de change par les chèques bancaires pour les paiements internationaux.

Le secteur financier résiste difficilement aux deux guerres mondiales mais reste l'outil indispensable pour sortir la Grande Bretagne du marasme économique. Cette perte de vitesse pousse néanmoins le Royaume-Uni à demander deux prêts colossaux au Fonds Monétaire International. Les mesures de libéralisation des marchés financiers prises par Margaret Thatcher en 1986, plus connues sous le nom de *Big Bang*, redynamisent considérablement la City et la replacent au centre des échanges économiques et financiers. Londres reste ainsi, en 2019, la première place financière au monde, malgré la montée en puissance des places financières asiatiques telles que Hong Kong ou Singapour.

Leader bancaire du vieux continent, le Royaume-Uni est ainsi très réactif lorsqu'il s'agit d'innover dans le secteur bancaire. L'arrivée des nouveaux moyens de paiement représente, néanmoins, un risque majeur que la puissance financière ne semble qu'avoir moyennement anticipé. Dans les nouveaux secteurs que sont les banques en ligne, les paiements sur le web, *le contact-less* ou encore les applications de paiement, le Royaume-Uni s'y est certes positionné. Néanmoins, ce nouveau terrain de jeu soulève de nouvelles problématiques concernant le contrôle et la protection des données bancaires. La digitalisation de l'économie a en effet entraîné l'apparition de nouveaux risques auxquels sont confrontés tous les acteurs de cette boucle, dont le nombre a drastiquement augmenté au cours de ce changement profond. Effectuer un paiement en ligne laisse de multiples traces pouvant être captées par divers acteurs durant l'acheminement des données. Ces données deviennent alors un enjeu majeur qui peut, selon le degré de maîtrise du pays, se transformer en un précieux avantage ou au contraire en une fuite catastrophique d'informations au profit d'acteurs économiques qui en auraient compris la portée stratégique.

Les relations étroites, que ce soit dans le domaine économique ou politique -notamment par le biais du renseignement- que le Royaume-Uni entretient avec les Etats-Unis depuis la fin de la Seconde Guerre mondiale, et la montée en puissance des acteurs économiques américains comme les GAFAs peuvent, dans ce nouveau contexte, représenter un réel risque pour le contrôle des données bancaires du Royaume-Uni. Le Brexit élargit par ailleurs cette menace aux citoyens européens, la stratégie de l'Union Européenne dans le domaine ne s'appliquant désormais plus au Royaume-Uni.

Il convient alors de s'interroger sur la stratégie mise en place par le Royaume-Uni, dans ce contexte mouvant et incertain, pour se munir d'outils adéquats de contrôle et de protection des données bancaires. Il s'agit, dans un premier temps, de dresser un état des lieux du système de paiement au Royaume-Uni (acteurs, anciens et nouveaux moyens de paiement) afin d'évaluer son degré d'indépendance stratégique sur ce secteur. Cette analyse conclut que la place des Etats-Unis dans le système bancaire du Royaume Uni est prépondérante et croissante (I). Il s'agira ensuite de présenter un panorama des dangers qui pèsent sur les données bancaires britanniques et de mesurer si la réponse du Royaume-Uni à ces menaces est suffisante et adéquate (II).

PARTIE 1 : Etat des lieux des moyens de paiement au Royaume-Uni

La Fintech et la révolution numérique sont venues complexifier l'écosystème des moyens de paiement dominé par le secteur bancaire depuis des siècles. Les infrastructures de réseau et leurs opérateurs ont su, malgré l'arrivée de nouveaux entrants dans le système de paiement, maintenir leur position prépondérante en s'assurant la dépendance des autres acteurs.

Chapitre 1 : Acteurs et fonctionnement du système de paiement britannique

Les banques et les opérateurs au cœur du système des moyens de paiement

Les moyens de paiement traditionnels regroupent les espèces, les chèques, la carte de paiement, le virement bancaire et le prélèvement bancaire et SEPA. Toutes ces fonctions sont à l'origine assurées par les banques et encadrées par des normes et réglementations.

Cinq banques majeures opèrent au Royaume-Uni :

- Barclays ;
- La Royal Bank of Scotland ;
- Lloyds ;
- Standard Chartered ;
- HSBC.

À elles seules, Barclays, HSBC et Lloyds possèdent 77% des comptes courants personnels britanniques et 85% des comptes d'entreprises selon une étude de la BNP¹. Les banques ne représentent cependant que la partie apparente du système de paiement, et font partie d'un ensemble plus large appelé prestataires de paiement. Mais qui permet de réaliser le paiement ?

Pour qu'un paiement se réalise il faut passer par un opérateur qui va utiliser un réseau pour effectuer ce paiement. Ainsi, l'opérateur de paiement dépend du fournisseur réseau, qui ne peut exploiter lui-même son réseau. Les trois principaux fournisseurs de réseau utilisés au Royaume-Uni sont Visa, Mastercard et Vocalink (filiale britannique de Mastercard)². Tous ces fournisseurs sont donc américains. Dans les opérateurs de paiement, on retrouve également l'influence américaine avec Visa Card Payments et Mastercard Payments mais également des systèmes de paiement britanniques : les Bacs, le Faster Payments System, le C&CCC et les

¹ NAHMIAS Laurent, « Les banques britanniques face au resserrement de la contrainte réglementaire », BNP-Paribas - Le portail des études économiques, Juin 2016

² PAYMENTS STRATEGY FORUM, « A Payments Strategy for the 21st Century: Putting the needs of users first », Novembre 2016, p.16

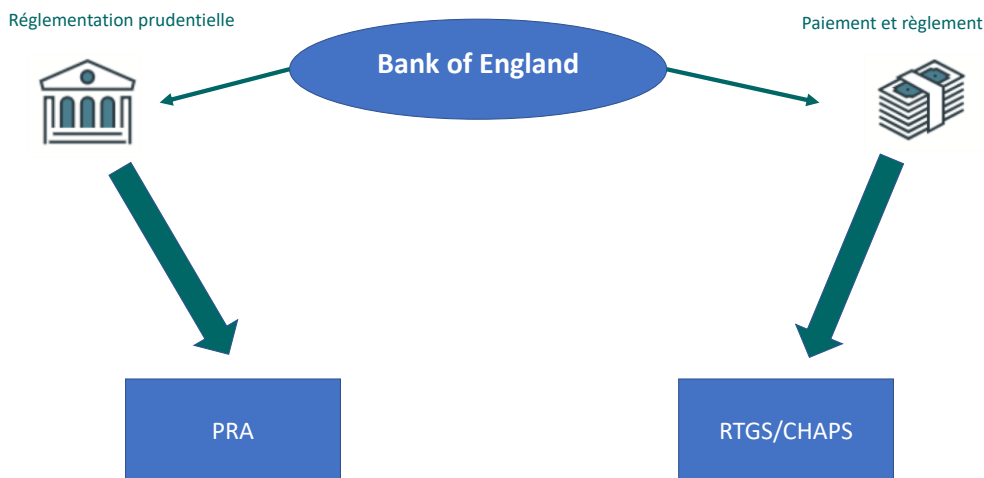
CHAPS. Les institutions financières font partie intégrante de la chaîne de fonctionnement du système de paiement du Royaume-Uni.

Les institutions financières au Royaume-Uni

Historiquement, les organismes privés et les institutions gouvernementales régissent conjointement le modèle financier britannique, dont le système de paiement national.

- 1- La Bank of England (BoE), banque centrale du Royaume-Uni, a été fondée en 1694. Cette dernière fut une société de droit privée durant plus de deux siècles avant d'être nationalisée en 1946. Elle devient, en 1998, un organisme public indépendant du gouvernement, contrôlée par le Trésor.

Le rôle de la Bank of England dans le système de paiement



Source : T. Buchmüller, B. David.

- **La Prudential Authority (PRA)**, organisme intégrant de la Bank of England créée en 2012, est chargée de la réglementation et de la surveillance prudentielle d'environ 1 500 banques, de sociétés de construction, de coopératives d'épargne et de crédit, d'assureurs et de grandes entreprises d'investissement. Celle-ci exige des sociétés financières qu'elles détiennent un capital suffisant et disposent de contrôles de risque. En outre, elle assure une étroite surveillance des entreprises quant à la gestion de leurs activités.

Les principaux objectifs de la PRA sont :

- Favoriser la sécurité et la solidité des entreprises ;
- Faciliter la concurrence entre elles ;
- Assurer un certain niveau de protection aux assurés.

- **Le système de paiement automatisé Clearing House (CHAPS)** est le système de paiement en temps réel et de grande valeur du Royaume-Uni, dans lequel les paiements sont effectués à travers le service de Règlement brut en temps réel (RGTS) de la Bank of England. Initialement créée en 1984, elle rejoint la BoE en novembre 2017. Cette dernière exploite désormais ce système de paiement. Outre les nombreuses institutions financières, les plus grandes entreprises effectuent des paiements CHAPS pour régler des opérations de marché monétaire, de change et de paiement de grande valeur.
- **Le service de règlement brut en temps réel (RGTS)** a été mis en place en 1996 pour permettre à différentes institutions, dont les banques principalement, de procéder à des paiements de diverses manières. Cette structure qui gère les comptes des sociétés de construction, des banques et des institutions, assure un transfert d'argent sans risque et en temps réel. Au Royaume-Uni, le système RGTS de la banque est l'un des principaux systèmes de paiement utilisés entre les banques membres et les institutions afin qu'elles puissent procéder au règlement de leur paiement. Une réelle prise de conscience quant à l'évolution des besoins des usagers, de la technologie et des diverses réglementations s'est effectuée ces dernières années, œuvrant à la création de nouvelles fonctionnalités et capacités au sein du système de paiement et de règlement, sur le point de se mettre en place.³ Ces nouveautés s'inscrivent en outre dans une logique d'amélioration de la résilience et de l'accès et surtout d'une gestion renforcée des risques qui en réalité, ne cessent de croître.

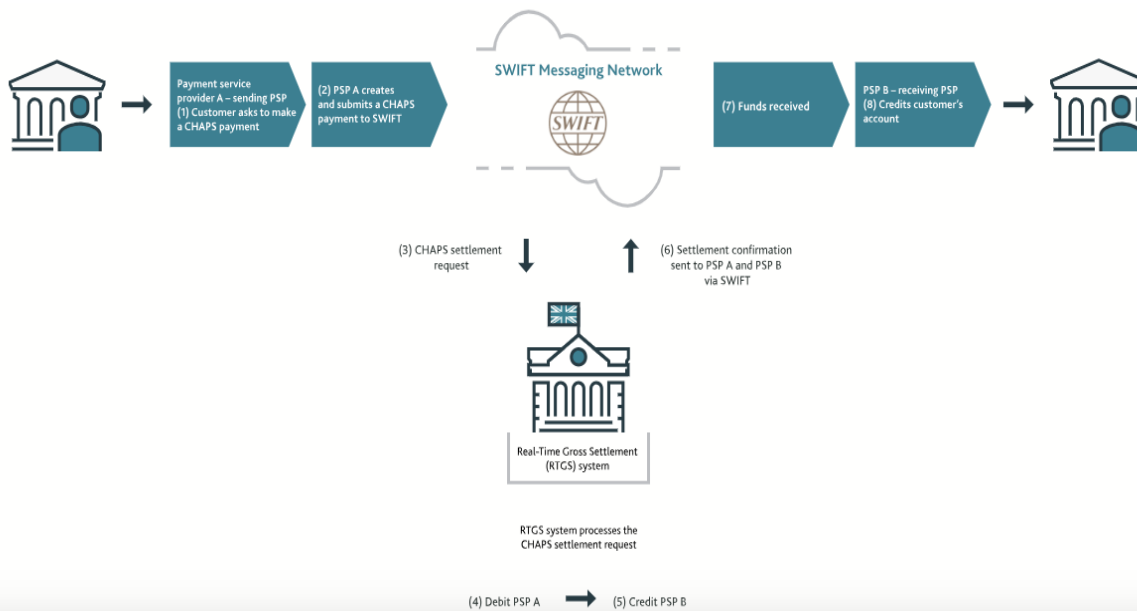
« For example, the Bank of England is in the midst of an ambitious rebuild of the Real Time Gross Settlement (RTGS) system – the backbone of every payment in the UK. »⁴

Mark Carney, gouverneur de la BoE

³ CARNEY Mark, « New Economy, New Finance, New Bank », BoE, 21 juin 2018

⁴ Ibid

Le système du CHAPS



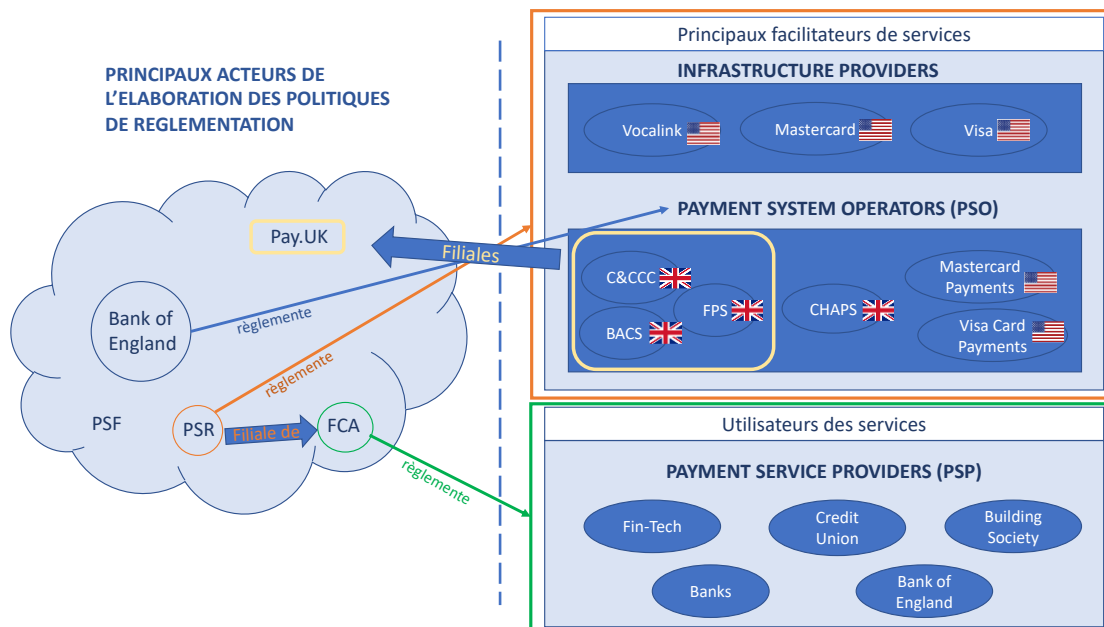
Source : Bank of England.

- 2- **La Financial Conduct Authority (FCA)** est une autorité de régulation du système financier au Royaume-Uni, indépendante du gouvernement britannique qui a succédé, en avril 2013, à la Financial Services Authority. Cette organisation a pour principal but de protéger les différents acteurs présents sur les marchés financiers, les particuliers et les différentes entreprises, afin d'assurer à tous un marché équitable. Elle se charge donc de veiller au bon fonctionnement des marchés financiers en matière de réglementation prudentielle, en promouvant une concurrence pertinente. Ses objectifs sont donc semblables à ceux de la Prudential Authority, cependant cette autorité est indépendante de la BoE.
- 3- **Payment Systems Regulator (PSR)**, est un organisme de réglementation des systèmes de paiement au Royaume-Uni, lancé en avril 2015. Cette filiale de la Financial Conduct Authority, « financée par l'industrie et responsable devant le Parlement »⁵ se voit, elle aussi, chargée de la concurrence et des pouvoirs de régulation. Elle veille à ce que tous les systèmes de paiement soient exploités afin de promouvoir une réelle et juste concurrence entre ces systèmes de paiements, leurs prestataires, les fournisseurs d'infrastructures et les opérateurs. En outre, celle-ci tend à impulser une dynamique de développement et d'innovation dans les systèmes de paiement et de leurs diverses infrastructures.
- 4- **Pay.UK**, est l'une des principales autorités de paiement de détail britannique. Celle-ci se charge désormais de l'exploitation de trois systèmes de paiement bancaire devenus ses filiales : **BACS Payments Schemes Limited**, **Faster Payments Scheme Limited** et de **The Check & Clearing Company**. Son objectif est de développer une économie dynamique en assurant une infrastructure ainsi que des normes de paiement de premier ordre. Grâce à tous ces services mis en place, Pay.UK assume à elle seule chaque jour 17,5 milliards de livres sterling de paiements.

⁵ Payment Systems Regulator, « The PRS Purpose », 2018

- **BACS** (anciennement Bankers Automated Clearing Services), est un système inter-bancaire créé en 1968 puis devenu en 2018 une filiale de Pay.UK, qui traite principalement du prélèvement automatique et du crédit direct BACS (paiement direct sur un compte bancaire ou sur un compte social).
 - **Faster Payments Scheme (FPS)**, désormais filiale de Pay.UK depuis 2018, a été mis en place en 2008 afin de garantir davantage de rapidité dans les délais de paiement et d'assurer ainsi en temps quasi réel des paiements et des ordres permanents. La plupart des paiements bancaires (Internet et téléphone) effectués au Royaume-Uni sont désormais traités par FPS.
 - **The Check & Clearing Company (C&CCC)**, filiale de Pay.UK depuis 2018, fondée en 1985, régit le système de compensation de chèques au Royaume-Uni.
 - **UK Payments**, fondée en 1985, est aujourd'hui une filiale de Pay.UK. Elle est spécialisée dans le secteur des paiements. Son objectif a été d'améliorer et d'innover le marché des services de paiement britannique en soutenant différents projets dont la création d'un service de paiement mobile (Paym), ou encore à travers la mise en place de paiements rapides et sécurisés (cartes à puce, codes Pin).
- 5- LINK** est le plus grand réseau de distributeurs automatiques de billets (environ 70 000 ATM) du Royaume-Uni. Fondé en 1985, il est désormais exploité par l'infrastructure de réseau VocaLink. En effet, VocaLink a été créée en 2007 par la fusion de Link Limited et de Voca Limited, désormais filiale britannique du groupe américain Mastercard.
- 6- SWIFT (Society for Worldwide Interbank Financial Telecommunication)** est une société coopérative mondiale créée en 1973 et basée en Belgique. Premier fournisseur mondial de services de messagerie financière sécurisée, elle dispose donc d'une plate-forme de messagerie et de nombreux services qui connectent plus de 11 000 organisations et infrastructures bancaires dans le monde.

Fonctionnement simplifié et principaux acteurs du système de paiement britannique



Source : T. Buchmüller, B. David.

Si les institutions et acteurs historiques demeurent des acteurs incontournables, de nouveaux acteurs émergent considérablement sur ce marché. La majorité de ces nouveaux acteurs se développent à travers la Fintech qui devient désormais un PSP non négligeable.

Chapitre 2 : La diversification des nouveaux moyens de paiement : l'entrée en force des GAFA et des Fintechs

Avec l'arrivée des nouvelles technologies et de la Fintech, le secteur bancaire a été fortement modifié et de nouveaux acteurs, ainsi que de nouveaux modes de paiement, sont apparus. Si la simplification d'utilisation est maître-mot de ces nouveaux modes de paiement, ils sont également venus ajouter de la complexité dans le processus de paiement : qui détient les données du consommateur ? Qui les gèrent et les utilisent ?

État des lieux des modes paiement en 2017

En 2017, 38,8 milliards de paiement ont été effectués au Royaume-Uni⁶. Les cartes de paiement restent le moyen le plus utilisé, notamment à travers l'utilisation du sans contact mais également lors des achats en ligne. En 2017, plus de 119 millions de cartes de paiement ayant

⁶ Une analyse plus détaillée de l'état des lieux est disponible sur : « UK Payment Market Summary 2018 », UK Finance, 2018

la fonctionnalité sans contact étaient en circulation. Ce type de paiement ne cesse d'augmenter et représente plus de 15% de l'ensemble des paiements effectués. Le paiement en espèces est en recul même s'il continue d'être utilisé pour 34% du total des paiements. L'utilisation du chèque est en baisse et représente une part insignifiante du marché. Le nombre de consommateurs utilisant les applications mobiles et les banques en ligne est en forte augmentation. Parmi les adultes britanniques, plus de deux tiers utilisent le service de banque en ligne et les applications mobiles des banques. Les autres moyens de paiement en ligne ou sur smartphone tels que Google Pay, Paypal, Apple Pay et Samsung Pay représentent une part grandissante du marché, voués à fortement augmenter dans les prochaines années.

Les acteurs des nouveaux modes de paiement et l'influence américaine

La révolution des modes de paiement s'est réalisée autour de plusieurs innovations : la technologie du QR code, la technologie RFID et NFC, et le paiement en ligne. Cela a permis à de nouveaux entrants de conquérir le marché et de devenir des acteurs à part entière du système de paiement.

Les cartes sans contact

L'adoption du sans contact au Royaume-Uni a eu lieu en 2015, lorsque les cartes de paiement sans contact ont été acceptées dans le réseau du métro londonien, permettant ainsi de réduire le temps d'attente aux tourniquets. Depuis l'été 2017, les cartes de paiement sont devenues le premier mode de paiement au détriment de l'argent liquide. A ce titre, les consommateurs britanniques sont particulièrement réceptifs à l'utilisation du sans contact : 30 % des paiements réalisés contre une proportion insignifiante aux Etats-Unis et dans d'autres pays européens⁷. Selon la UK Card Association, en avril 2017, 3,9 milliards de livres sterling ont été dépensées au Royaume-Uni en utilisant la technologie sans contact de la carte de paiement, soit une augmentation de 147,6% par rapport au même mois l'an passé.⁸ Les cartes de paiement sans contact permettent de payer des articles sans entrer le code PIN à l'aide de la technologie de communication sans fil NFC (Near-field Communication) qui permet à un appareil de communiquer avec un autre.

Les principaux fournisseurs de cartes sans contact restent Visa et Mastercard qui proposent leur carte de paiement sans contact à travers les banques britanniques.

Les applications mobiles

Selon le Center for Economic and Business Research, 20 millions d'adultes utiliseront leur téléphone portable pour payer leurs biens et services d'ici la fin de la décennie, la valeur des achats triplant par rapport au niveau actuel pour atteindre £14,2 milliards en 2018.⁹ Les applications mobiles sont un ensemble très hétérogène. Certaines utilisent la technologie du NFC à l'instar des applications des GAFAs, d'autres se sont développées autour du QR code.

⁷ ANUSIC Ingrid, « Will 2018 be the year of contactless payments in the US ? », 14 février 2018

⁸ Louis Peake, « The rise of contactless cards in the UK », Finextra, 21 Mai 2018

⁹ CEBR, « Mobile Payments to boost UK economy », 5 novembre 2013

Enfin, au Royaume-Uni, les banques sont également très impliquées dans ce secteur. Ainsi, l'application de paiement par numéro de téléphone Pingit a été lancée par Barclays, banque emblématique britannique. Les applications émanant des GAFAs telles que Apple Pay ou encore Google Pay utilisent la technologie du NFC pour payer. Pour cela, ils demandent au préalable les coordonnées de la carte de paiement pour pouvoir utiliser la technologie sans contact intégrée au téléphone. Ces données bancaires deviennent alors propriété des GAFAs. Samsung Pay, émanant du Chaebol coréen Samsung, fonctionne de la même manière.

Les fournisseurs d'infrastructure ont également cherché à conquérir cette nouvelle opportunité. Ainsi, Vocalink, filiale britannique de Mastercard, a développé au Royaume-Uni à travers Zapp, son application PaybyBank. Celle-ci offre un accès direct au compte bancaire pour effectuer des paiements rapides et sécurisés via un smartphone. PaybyBank entre en concurrence directe avec les cartes de paiement et apparaît comme un moyen de paiement en ligne aux côtés de celles-ci. HSBC, Barclays, la Bank of Scotland, Lloyds ou encore Halifax utilisent Paybybank dans leurs applications mobiles.

Enfin, le PSR (Payment Systems Regulator) a développé une application permettant de lier directement le numéro de téléphone à un compte bancaire : Paym. Cette application britannique semble donc être une alternative. Cependant, si l'on remonte la chaîne de fonctionnement du système de paiement, le fournisseur de réseau utilisé n'est autre que Vocalink.

Ainsi, quelles que soient l'application et la nouvelle technologie utilisées, les fournisseurs de réseaux restent des acteurs incontournables dans le système de paiement.

Les banques en ligne, les banques digitales et l'arrivée d'Amazon Web Service au Royaume-Uni

L'arrivée des banques en ligne a permis à des acteurs externes au système de paiement de s'intégrer dans le processus. Ainsi, Tesco, groupe de distribution internationale, a pu créer sa propre banque en ligne : Tesco Bank.

L'année 2016 a connu le lancement de nouvelles banques digitales, avec l'octroi d'une licence bancaire de la part de la FCA. Ces nouvelles banques digitales ont la particularité de s'utiliser uniquement via une application mobile. Monzo, Atom ou encore Starling Bank font partie de cette nouvelle catégorie. Si ces nouvelles banques sont britanniques, les cartes de paiement, utilisées ne sont autres que des cartes Visa et Mastercard. Encore une fois, les nouveaux acteurs du système de paiement ne peuvent se passer des entités américaines.

La révolution du numérique, la volonté de créer des applications et des services en ligne ont également attiré un autre acteur dans le système : Amazon Web Service (AWS). AWS, appartenant au groupe américain Amazon, offre un service de cloud computing à la demande pour les entreprises et les particuliers. AWS propose de nombreux services allant du stockage des données à la gestion d'applications mobiles et à la gestion de système. Ses services sont utilisés par l'ensemble des acteurs du système de paiement. Monzo et OakNorth, des banques

numériques récentes, l'utilisent. Sur le site d'AWS¹⁰, on y trouve le fait que la banque Oak-North utilise l'entité pour maintenir sa sécurité et sa conformité. Des banques « historiques », telle que HSBC, sont également clientes d'AWS : HSBC s'en sert pour la conception d'applications mobiles.

Les prestataires de service du paiement en ligne

Le paiement en ligne a introduit une concurrence directe aux banques. Alors que le système alimente les banques (transfert de monnaie bancaire vers compte non bancaire), il les fait également entrer en concurrence (paiements des transactions entre membres du système en compte non bancaire). Ce mode de paiement a permis l'émergence d'un nouvel acteur : les prestataires de service de paiement en ligne. Cela ajoute ainsi de la complexité dans le système de paiement pour savoir qui détient les données du consommateur.

Parmi les principaux prestataires de service de paiement implantés au Royaume-Uni, Worldpay est de loin le plus utilisé, gérant plus de 40% des transactions par carte. Cette société, dont le siège social est installé au Royaume-Uni, a en réalité comme sociétés mères deux fonds d'investissement et de gestion américains. Shopify, le deuxième prestataire le plus utilisé est quant à lui canadien. Paypal est également un acteur important des PSP bien que le service ne soit que le troisième moyen utilisé au Royaume-Uni. Enfin, Stripe, société américaine d'origine irlandaise, s'impose également comme un acteur emblématique des PSP dans le pays.

D'autre part, les prestataires de services de paiement en ligne basés aux Etats-Unis sont régis par le Financial Crimes Enforcement Network, qui dépend lui même du Trésor américain. L'organisme a l'autorisation de collecter et d'analyser les informations issues des transactions financières. L'objectif officiel est de lutter contre le blanchiment d'argent, le terrorisme et autres crimes financiers.

Ainsi, quel que soit le mode de paiement utilisé, les données sont souvent transférées à des sociétés américaines. Si Visa et Mastercard détiennent historiquement et économiquement le marché britannique, les GAFAs et les prestataires de paiement en ligne, américains pour la majorité, ont su néanmoins s'imposer en devenant de nouveaux acteurs emblématiques du système de paiement.

¹⁰ Amazon Web Service, « AWS Case Study: OakNorth Bank », Site web AWS, 2018

PARTIE 2 : La mise en œuvre d'une stratégie nationale limitée

Le marché des systèmes de paiement dans le monde a été fortement impacté par les avancées technologiques fulgurantes dans les domaines du stockage, de la collecte et du traitement de la donnée. De nouveaux logiciels sont désormais capables de déterminer des tendances par l'analyse d'une quantité massive de données (le « *Big data* »), c'est-à-dire un volume si élevé qu'un individu ne peut matériellement traiter seul. Au Royaume-Uni, l'accès au « *Big data* » (qui s'est élargi grâce à une baisse des coûts des logiciels de traitement) et la mise en place d'une réglementation adaptée, ont poussé les nouveaux acteurs de la Fintech à tirer parti de cette technologie de rupture pour se positionner sur le marché des nouveaux moyens de paiement. En fondant leur *business model* sur le traitement de la donnée, ils sont en passe de refonder en profondeur un marché historiquement acquis aux banques et de transformer les habitudes de paiement des individus. Pour l'organisme de régulation des paiements britannique, le PSR, l'entrée de la donnée comme enjeu stratégique et commercial pour les entreprises et les banques, a déclenché une « *rapide évolution dans les services de paiement* » qu'il s'agit de soutenir¹¹.

L'arrivée de nouveaux acteurs sur le marché des moyens de paiement a néanmoins facilité la captation illégale des données des utilisateurs. La multiplication des acteurs par qui transite la donnée a ainsi augmenté la vulnérabilité de la chaîne de transmission des données entre le payeur et son bénéficiaire.

Chapitre 1 : Un système à la vulnérabilité grandissante

Des failles renforcées par l'élargissement de la chaîne de transmission des données

¹¹ Payment Systems Regulator (PSR), « Discussion paper: Data in the payments industry », Juin 2018, p.11

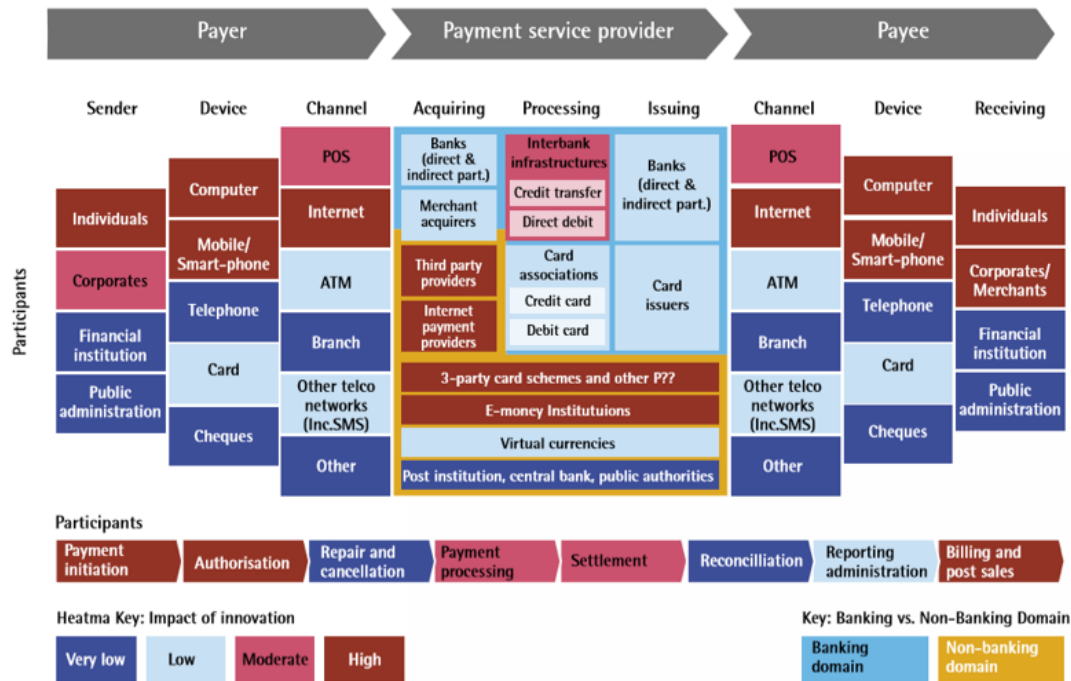
La numérisation des données, par l'exposition des données qu'elle implique, entraîne une augmentation des risques liés à leur stockage et leur utilisation. Lors d'un paiement sur internet, l'utilisateur s'expose à de multiples captations de données potentielles ainsi qu'au risque cyber de manière plus générale.

EN AMONT	PENDANT	APRÈS
Son système d'exploitation	Son réseau	Banque de données
Son navigateur	Son point de connexion	Réseau
L'exposition au phishing	Son fournisseur internet	Messagerie si confirmation de paiement / envoi de facture
Les applications	Les nœuds de connexion	Téléphone si confirmation de paiement / envoi de facture
	Les câbles sous-marins	
	Son pair (particulier ou entreprise)	

Les données captées légalement ou illégalement peuvent porter atteinte à la vie privée de l'utilisateur. Si le paiement sur Internet est réalisé par le biais d'un objet connecté, le risque cyber est accru. Il convient donc de s'interroger sur la manière dont les acteurs de ce cycle de paiement connecté peuvent avoir accès aux données des utilisateurs : quelles données et où sont-elles stockées ?

Le système d'exploitation, quelque soit son support (ordinateur, téléphone ou tablette), récolte des données. Certaines applications installées peuvent aussi être vecteurs de fuites d'informations lorsqu'elles ont accès à des données privées. L'utilisation d'un navigateur internet pour accéder au paiement entraîne une faille supplémentaire. Premièrement, le navigateur garde en mémoire l'historique de navigation effectuée sur le web. En sus de cela, l'utilisateur peut éventuellement être victime d'un site de phishing spécialisé dans la récolte d'identifiants, de données bancaires, ou les deux. A ce stade, l'utilisateur est aussi confronté au problème de la sécurité du réseau ainsi qu'à celui de la fiabilité de l'opérateur. Enfin, l'acheminement entier de l'information comporte d'importantes failles, que ce soit le point de connexion, les nœuds ou encore les câbles sous-marins sans lesquels il ne serait pas possible de faire transiter l'information à une telle vitesse.

Chaîne de transmission de la donnée dans le système de Paiement : une multiplicité d'acteurs



Source : Rapport de Accenture : Review of the International Landscape of Innovation in Payments and Insights for UK Payments, 2014.

Selon une étude de SagePay datant de 2017, 81% des personnes interrogées dans le cadre d'une enquête de YouGov¹² se sentent inquiètes à propos de la sécurité de leurs données dans le cadre d'un paiement à partir d'un mobile. Cette statistique n'a pas chuté au cours des 12 derniers mois, malgré des mesures prises par les différents tiers pour rassurer les clients. Une autre étude¹³ confirme ces premières statistiques, montrant que 70% des interrogés s'interrogent à propos de la sécurité des nouvelles technologies de paiement.

Le Royaume-Uni : mauvais élève de la cybersécurité

Bien que le coût des cyberattaques au Royaume-Uni ait diminué en 2017, les pertes financières s'élèvent à 1,1 millions de dollars et ce sans compter la perte colossale de données. De fait, les données clients ont été compromises dans 25 % des cas. Le Royaume-Uni est peu préparé face aux cyber attaques. Les entreprises britanniques victimes d'attaques reprennent, en moyenne, le contrôle de leur système en 19 heures. Par ailleurs, seulement 44% des entreprises britanniques ont mis en place une politique de sécurité. En 2017, le ransomware WannaCry a fortement impacté le Royaume-Uni, avec comme victime principale, le National

¹² SagePay, « 2017 Payment Landscape Report », 2018

¹³ SagePay, « 2017 Payment Landscape Report », 2018

HealthService (NHS)¹⁴. Cette attaque aura permis d'éveiller les consciences sur l'importance de l'application des bonnes pratiques en matière de sécurité informatique. Affaibli de son expérience en cyberattaque, un plan stratégique portant sur la période 2016-2021¹⁵ a été lancé par le gouvernement dans le but de sécuriser les connexions des objets et infrastructures de l'internet des objets (IoT).

L'attaque subie par British Airways à la fin de l'été 2018 met en exergue la vulnérabilité persistante du Royaume-Uni quant aux cybermenaces¹⁶. En l'espace de quinze jours, la compagnie aérienne britannique indique avoir été victime d'une cyberattaque portant sur les données de 380 000 cartes de paiement de ses clients¹⁷.

¹⁴ National Audit Office, « Investigation : WannaCry cyberattack and the NHS », National Audit Office, 24 octobre 2017

¹⁵ Cabinet Office, National Security and Intelligence, HM Treasury and The Rt Hon Philip Hammond MP, « National Cyber Security Strategy 2016 to 2021 », Gov.uk, 1^{er} novembre 2016

¹⁶ ZAGHET Camille, « Le Royaume-Uni manque considérablement de préparation contre les cyberattaques », Siecle Digital, 19 novembre 2018

¹⁷ COUNIS Alexandre, « British Airways victime d'un vaste piratage informatique », Les Echos, 6 septembre 2018

Chapitre 2 : Face à une stratégie de libéralisation des données, un contrôle suffisant des données ?

Face à l'arrivée des nouveaux acteurs et de nouvelles technologies de plus en plus intrusives pour la vie privée, le Royaume-Uni a mis en œuvre une stratégie nationale double. Il s'agit de moderniser le système des paiements et de produire une législation adaptée (Open banking) pour tirer profit des avancées technologiques. Le RGPD, apparaît à ce titre, comme un garde fou, permettant d'éviter des dérives liées à ces changements structurels.

La Nouvelle Architecture des paiements : une stratégie nationale de modernisation des systèmes de paiement et de libéralisation du partage de données

En 2015, à l'instigation du Payments Systems Regulator (PSR), a été lancé le *Payments Strategy Forum* (PSF), une initiative qui a réuni les acteurs de l'écosystème des paiements au Royaume-Uni (banques, agences de régulation, entreprises de la Fintech) pour penser la transformation de ce marché. Ce Forum a produit en 2016 un document de stratégie nationale visant à mettre en œuvre la *Nouvelle Architecture des Paiements* (New Payments Architecture -NPA). Il s'agit d'une refonte complète de l'écosystème des paiements du pays permettant au Royaume-Uni de faire face aux nouveaux défis posés par l'arrivée de nouvelles technologies et des nouveaux acteurs qui les accompagnent¹⁸. Sous la supervision du PSR et de la *Bank of England*, le nouvel opérateur de systèmes de paiement, *Pay.UK* (anciennement NPSO), est en charge de la mise en œuvre de la stratégie qui ne débutera qu'à l'horizon 2021.

La stratégie britannique des paiements comporte trois axes principaux : (I) la mise en œuvre de nouvelles formes de paiement qui correspondraient aux besoins des consommateurs et des entreprises ; (II) la lutte contre la fraude ; et (III) la simplification de l'écosystème des paiements pour relancer la concurrence et encourager l'innovation. L'atteinte de ces objectifs contribuerait, à terme, à la fondation d'une nouvelle architecture des paiements¹⁹.

L'utilisation de la donnée est au cœur des nouvelles formes de paiement soutenues par le *Payments Strategy Forum*. Le mécanisme « *assurance data* » permettrait, par exemple, de fournir des informations à un payeur concernant son bénéficiaire avant et après une transaction bancaire. Ce mécanisme permettrait de vérifier l'identité du bénéficiaire et répondrait ainsi aux besoins exprimés par les consommateurs d'avoir « *plus de contrôle* » sur leurs transactions bancaires. Le mécanisme « *enhanced data* » permettrait, quant à lui, de lier des données à un paiement électronique. Cela permettrait à l'utilisateur d'identifier rapidement le paiement sans devoir attendre les informations supplémentaires qui sont d'habitude envoyées séparément par mail, et plus généralement, de fluidifier le système de transactions bancaires.

¹⁸ BURKITT Henry, « New payments architecture : the next big innovation in payments », *Out Law*, 6 juin 2018

¹⁹ Payments Strategy Forum, *A Payments Strategy for the 21st Century: Putting the needs of users first*, Novembre 2016, p.9.

L'enjeu de la sécurisation des données liées à ces nouveaux moyens de paiement n'a été que partiellement traité. Lors de la Consultation du Forum le 31 juillet 2017, ses membres reconnaissent que des risques liés à l'utilisation des données ou à leur stockage existaient²⁰ mais sans apporter de détails ni de solutions mis à part la nécessité de conformité avec la législation européenne notamment le RGPD, le PSD2 et la directive de l'Union européenne contre le blanchiment d'argent²¹.

Le deuxième axe de la Nouvelle Architecture des Paiements (NPA), qui vise à lutter contre la fraude, se base sur la centralisation des données de paiement des utilisateurs au sein d'un « *global dataset* » ce qui pose la question de la sécurisation des lieux de stockage des données et de leur accès.

Quant au troisième axe du NPA, qui vise à redynamiser la concurrence dans le marché des moyens de paiement et à relancer l'innovation, des mesures sont en cours pour permettre à des acteurs non bancaires de pouvoir ouvrir des comptes au sein de la Bank of England et donc de se positionner sur le marché des systèmes de paiement²². Il s'agit là d'un réel coup de pouce réglementaire octroyé aux entreprises anglaises de la Fintech. Le soutien aux Fintechs a été érigé en priorité par le gouvernement. Le Royaume-Uni est aujourd'hui pionnier dans le secteur des paiements des entreprises Fintechs : ce marché représente à lui seul 10 milliards de livres par an, soit 50% du marché total des Fintechs dans le pays²³. Selon une étude de EY, ce marché possède de nombreux atouts de croissance, dont notamment une réglementation et un environnement des affaires très favorables. Ce cercle vertueux a conduit à la naissance d'entreprises innovantes, telle que l'application Moneybox, société anglaise dont le siège social se trouve à Edimbourg. En 2018, cette Fintech anglaise devient le premier fournisseur de services de paiement proposant à ses clients une intégration à Santander.

Par ailleurs, pour faciliter l'accès au marché, les différents opérateurs de systèmes de paiements ont été récemment regroupés au sein d'une seule et même instance, Pay.UK, ce qui permet d'harmoniser la réglementation. La nécessité d'harmonisation a également conduit le *Payment Strategy Forum* à soutenir la mise en place de la norme de messagerie ISO 20022 dans les systèmes de paiement CHAPS, Faster Payments et Bacs²⁴. Cette nouvelle messagerie

²⁰ BURKITT Henry, « New payments architecture : the next big innovation in payments », Out Law, 6 juin 2018

²¹ Out Law, "Interoperable systems and data at the heart of plans to modernize UK payments infrastructure", 31 juillet 2017

²² Payments Strategy Forum, A Payments Strategy for the 21st Century: Putting the needs of users first, Novembre 2016, p.49.

²³ Landscaping UK Fintech. Commissioned by UK Trade & Investment, EY, 2014, p.7.

²⁴ Interview de CLELAND Victoria, La Banque d'Angleterre se prononce sur le renouvellement du système de règlement brut en temps réel (RBTR) et sur les répercussions de la norme ISO 20022, sur Paiements Canada.

utilisera encore davantage les données des utilisateurs en rendant obligatoire, au sein du message, l'identification du payeur et l'objet de la transaction bancaire en question²⁵. Selon Victoria Cleveland, directrice générale des paiements bancaires de la Bank of England, l'utilisation de plus d'information dans la nouvelle messagerie permettrait de lutter contre la fraude.

L'argument du besoin d'accélérer l'innovation a, par ailleurs, été récemment invoqué par l'organisme britannique de réglementation (PSR), pour lever les restrictions sur le partage de données entre le fournisseur d'infrastructures principal du NPA²⁶ et les fournisseurs de services. Cette mesure, qui est à l'étude depuis juillet 2018, obligerait le fournisseur de services principal à partager de manière sécurisée les données bancaires avec les fournisseurs de services. Selon le PSR, « *cela pourrait ressembler en principe aux obligations de partage de données du PSD2 et de l'open banking* »²⁷. Restreindre le partage des données de paiement représenterait, selon le PSR, une barrière à l'innovation. La réticence des consommateurs concernant un accroissement du partage de leurs données de paiement a été identifiée, mais celle-ci est perçue comme une « *barrière supplémentaire potentielle à la concurrence et à l'innovation* » qui nécessite d'être levée par la mise en œuvre de campagnes de réassurance.

Plus généralement, pour le PSR, la législation de protection des données s'applique uniquement aux données personnelles (c'est-à-dire des données qui permettent d'identifier une personne). La loi de protection de données ne s'applique pas aux entités privées (entreprises)²⁸. Le PSR souligne aussi que l'organisme chargé de la protection de données est l'Information Commissioner's Office (ICO) et que la législation en vigueur sur la protection des données (RGPD et le Data Protection Act 2018) doit être respectée.

A la stratégie générale de modernisation des systèmes de paiement, s'ajoute une initiative spécifiquement basée sur la libéralisation du partage des données de paiement. Amorcée par le NPA, elle devient l'épine dorsale de la loi dite *Open banking*.

L'Open Banking : la mainmise des acteurs non-bancaires sur les données des transactions bancaires du Royaume-Uni

Concernant l'accès à la donnée, les banques britanniques étaient jusqu'à présent en situation de force face aux consommateurs et aux entreprises commerciales. Cette position s'est construite autour de la détention des données les plus précieuses et les plus sensibles du monde : les détails des transactions des consommateurs. Connaître les habitudes de consommation, les régimes alimentaires, les choix de lieux de vacances, les loisirs et en définitive, le niveau de vie des utilisateurs représente un avantage concurrentiel considérable auxquelles seules

²⁵ Payment Systems Regulator (PSR), Discussion paper: Data in the payments industry, DP18/1, Juin 2018, p.24

²⁶ Il n'a pas encore été choisi par Pay.UK. Un appel d'offres a été lancé en octobre 2018 et devrait se clôturer en 2021.

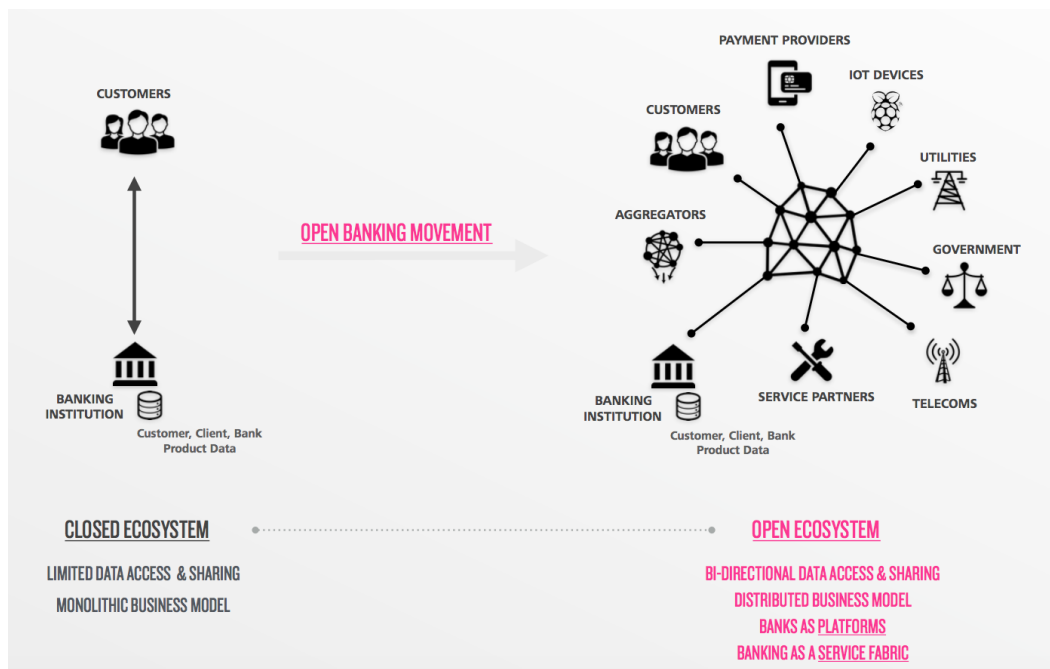
²⁷ Out Law, « UK regulator considers opening up access to data from payment systems », 2 juillet 2018

²⁸ Payment Systems Regulator (PSR), Discussion paper: Data in the payments industry, DP18/1, Juin 2018, p.8.

les banques pouvaient avoir accès. D'autres données importantes sont soigneusement conservées par les banques tels que les détails exacts des découverts, des cartes de crédit, des prêts et des hypothèques ainsi que des produits financiers qui ont un impact sur la vie de millions de personnes.

Suite à la deuxième directive sur les services de paiement (DSP2), le Royaume-Uni a mis séparément en place l'Open Banking. Cette loi vise à ouvrir le marché de la banque de détail en s'alignant sur la législation de l'Union Européenne. Instauré le 13 janvier 2018 et imposé par la Competition and Markets Authority (CMA) du Royaume-Uni, l'Open Banking pourrait redistribuer les cartes dans la maîtrise des données de paiement. En outre, cette dernière répond à une stratégie nationale permettant de relancer la compétitivité des banques de détail et d'encourager l'innovation. Dans ce cadre, l'Open Banking permet à toutes ces données stratégiques d'être rendues plus accessibles notamment aux entités non bancaires. Celles-ci doivent être agréées par la Financial Conduct Authority (FCA)²⁹ afin d'accéder aux données des transactions en compte courant détenues, jusqu'à présent, exclusivement par les banques.

L'Open Banking, un accès élargi aux données de paiement



Source : Deloitte analysis³⁰

L'Open Banking : un outil d'influence redoutable

L'Open Banking s'applique actuellement aux banques traditionnelles telles que Barclays, HSBC, Lloyds et Royal Bank of Scotland qui contrôlent 77% du marché national des comptes courants mais aussi la Allied Irish Bank, Santander, la Danske, la Lloyds et la Nationwide. Ce

²⁹ LEVINSON Matthew, European banks brace for shake-up in customer data access, Financial Times, 11 janvier 2018

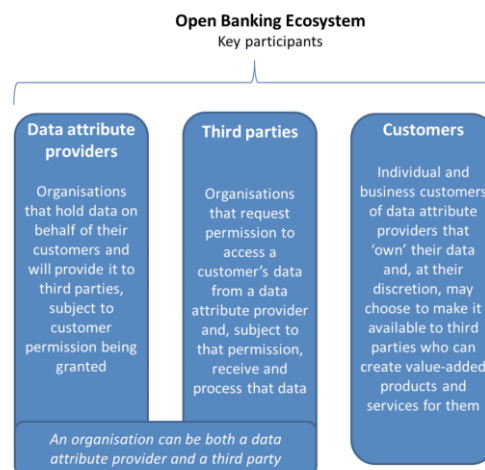
³⁰ Deloitte, « Open Banking and PSD2 : How to flourish in an uncertain future », 2018

système met donc en place le partage de données relatives aux comptes courants des consommateurs avec des sociétés non bancaires (appelées fournisseurs tiers ou TPP). Ainsi, les informations de comptes relatives aux différentes banques d'un même utilisateur seraient stockées et disponibles de manière centralisée aux acteurs bancaires comme aux acteurs non-bancaires. Aujourd'hui, la plupart de ces tiers sont des startups issues du domaine de la Fintech. L'Open Banking représente un outil d'influence redoutable pour le Royaume-Uni afin d'exporter ses Fintechs nationales vers les marchés étrangers, de se positionner comme leader de ce système disruptif et, *in fine*, d'opérer « *une colonisation par les normes* ». A titre d'exemple, l'Australie adoptera l'Open Banking en juillet 2019³¹ : l'opportunité pour le Royaume-Uni d'introduire ses acteurs non-bancaires susceptibles d'être acceptés par les banques australiennes comme fournisseur tiers.

Les données de transactions bancaires : nouveau produit des Fintechs

L'Open Banking part du constat que le secteur bancaire n'a pas su tirer profit des avancées technologiques du numérique. Courant 2019, la CMA pourra également solliciter les fournisseurs de cartes de crédit, de portefeuilles numériques et de cartes prépayées pour partager des données dans le cadre de l'Open Banking, au même titre que les banques. Tirant parti de cette nouvelle législation, plusieurs startups du marché du Royaume-Uni telles que Moneybox, Monzo, ou encore Yolt commencent à développer des applications et des services qui exploitent les données bancaires. D'autres acteurs peuvent tirer leur épingle du jeu telles que les Fintechs américaines TrueLayer, Plaid et Finicity³². En tant que plates-formes API, elles offrent aux développeurs un moyen d'accéder aux données bancaires dont ils ont besoin pour créer de nouvelles applications et services financiers.

Les acteurs de l'Open Banking



Source : Payments Strategy Forum³³

³¹ BLOCH Valeska, SMITH Gavin, HIGGINS James, HALL Claudia, ORTNER Alex, Australia moves to Open Banking in 2019, Linklaters, 19 novembre 2018

³² BRODSKY Laura, IP Chris, and LUNDBERG Tobias, « Open banking's next wave: Perspectives from three fintech CEOs », Mc Kinsey, août 2018

³³ Open Banking Working Group (OBWG), « The Open Banking Standard : Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation », 16 février 2016

Présentée comme un moyen d'améliorer la concurrence au sein du secteur des banques de détail et l'ouverture à de nouvelles opportunités de marchés, cette nouvelle régulation de paiements va en réalité impliquer une concurrence mondiale entre les acteurs historiques du système bancaire, et les nouvelles Fintechs. L'Open Banking représente donc une aubaine pour les géants américains de la technologie tels que Facebook et Google. L'accès aux transactions bancaires du consommateur leur permettraient d'effectuer un traçage toujours plus précis des habitudes d'achats, afin de proposer des produits et services extrêmement ciblés en fonction du profil établi. Cette ouverture des GAFA aux opérations bancaires mais également aux startups qu'ils pourraient financer, menace les banques traditionnelles de perdre leur monopole dans le domaine. En effet, les GAFA tentent depuis longtemps de percer dans le secteur des services financiers, avec des produits tels que Pay by Messenger, Apple Pay et Google Wallet. Jusqu'à présent, ces efforts n'ont pas porté leurs fruits au Royaume-Uni, tant le secteur bancaire est réservé aux acteurs historiques. De leur côté, les processeurs de carte de paiement comme Visa et Mastercard se préparent également à se placer comme acteurs majeurs de l'écosystème de l'Open Banking.

« Imagine if your bank was as novel and innovative as a smartphone maker that diligently creates a whole new device every year. Imagine if you expected as much from your bank account as a new iPhone or Galaxy. ³⁴ »,
Sebastian ANTHONY, Bankrate UK

La multiplicité des acteurs : des risques de cybersécurité décuplés

En vue de l'accès des sociétés commerciales aux données bancaires des consommateurs - après avoir donné leur consentement- ce système présente des risques considérables en termes de sécurité et de respect de la vie privée. Lorsqu'un consommateur se connecte sur l'application de sa banque, il accepte ou non de transmettre ses données de transaction à une autre application non bancaire (le fournisseur tiers) qui a été validée au préalable par la Financial Conduct Authority (FCA). Le consommateur choisit le niveau d'accès ainsi que le temps de partage de ses données. Sa banque transmet ensuite les données convenues à l'application non bancaire via l'ouverture de son interface de programmation applicative (API). Cette circulation plus libre des données via l'ouverture des APIs bancaires aux applications non bancaires (Apple Pay par exemple) implique une augmentation des risques de cybersécurité. Parmi eux, des risques accrus de phishing via des courriers électroniques, des messages texte, des notifications ou de toute autre correspondance invitant le consommateur à cliquer sur un lien ou à fournir des données personnellement identifiables.

Dans ce contexte de révolution numérique, le Royaume-Uni adopte une forte stratégie de libéralisation de la donnée. Par l'entremise de l'Open Banking, le Royaume-Uni a su exploiter la valeur stratégique de la donnée bancaire pour se positionner sur le nouveau marché de la

³⁴ ANTHONY Sebastian, « What is Open Banking, and is it safe ? », Bankrate UK, 27 mars 2018

Fintech afin de construire une puissance numérique britannique. Le rôle de la Financial Conduct Authority (FCA) s'avère crucial dans la sélection des tiers non bancaires éligibles au partage des données. Ainsi, ce mécanisme permet au Royaume-Uni de se protéger d'une domination étrangère.

En somme, l'Open Banking est un système disruptif qui retire aux banques leur statut monopolistique sur les données de transactions. Ce système révolutionnaire incite les banques à réagir activement et à se réformer. L'arrivée des cryptomonnaies a également bouleverser le système bancaire qui, à l'inverse d'une transparence de l'accès aux données, permet de décentraliser et anonymiser les transactions.

Les cryptomonnaies : une technologie de rupture

« Free yourselves from the current burden we all share : a government that was created to serve us than has instead become our master. How ? By replacing the system used to control us – currency – with a system that we, the citizens control : Cryptocurrencies ».

John McAfee³⁵ le 18 Décembre 2018

Au Royaume-Uni, la cryptomonnaie questionne et fascine l'Etat³⁶. Le gouvernement britannique ne cache pas sa méfiance et sa fascination pour les cryptomonnaies.

Pour ce faire, l'île n'hésite pas à investir drastiquement dans le secteur de la Fintech. Philip Hammond, homme politique et chancelier de l'échiquier britannique, estime qu'il y a « *des projets pilotes visant à aider les nouvelles entreprises de fintech, et plus largement l'industrie des services financiers, à se conformer à la réglementation en construisant des logiciels qui leur permettraient de suivre automatiquement les règles. Leur permettant ainsi d'économiser du temps et de l'argent* ».

La blockchain intéresse, mais qu'en-est-il pour les cryptomonnaies ? Est-ce un moyen de paiement régulé ? Peut-on le contrôler ? *Quid* de la souveraineté de l'État et des données ?

Tout d'abord, il existe une différence fondamentale entre les monnaies électroniques et la cryptomonnaie. Les monnaies électroniques ont existé depuis les prémices de l'internet. Il s'agit d'« *une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* »³⁷ A titre d'exemple, les

³⁵ Informaticien anglais, fondateur du logiciel McAfee, principal influenceur pro-cryptomonnaie

³⁶ WILLIAMS-GRUT, « Oscar, Britain is getting a cryptocurrency taskforce », Business Insider, 22 Mars 2018

³⁷ Loi n 2013-100 du 28 Janvier 2013 – art.5

applications mobiles qui stockent et émettent de l'argent, utilisent des monnaies électroniques, puisque les deniers sont dématérialisés. Les cryptomonnaies, quant à elles, sont basées sur le cryptage et sur le système de la blockchain.

Les cryptomonnaies remettent en cause un système centralisé : un système bancaire où les flux financiers transitent depuis l'avènement des Médicis. La cryptomonnaie apparaît donc comme une alternative qui permet de s'affranchir de cette dépendance. L'État et les banques ont saisi les enjeux liés au développement d'une telle technologie. Face à la vague des cryptomonnaies, la seule mesure que les États occidentaux ont pu mettre en place est de définir le bitcoin comme un actif assujéti à la taxe sur les plus-values financières³⁸ (28% de taxe d'imposition au Royaume-Uni).³⁹

Dès lors, il n'a pas fallu très longtemps pour que chaque État prône la création de sa propre cryptomonnaie.⁴⁰ Ainsi, prenant exemple sur son voisin scandinave, la Suède, qui prévoit de lancer un programme de monnaie numérique le E-krona, le Royaume-Uni ambitionne de créer sa propre cryptomonnaie⁴¹. Les enjeux sont considérables, le Royaume-Uni se doit de surfer sur la vague des cryptomonnaies afin d'être compétitif dans un monde hyper-numérisé. Mais *quid* des données ?

A *contrario* des flux financiers classiques, les cryptomonnaies utilisent la technologie de la blockchain. Cette technologie permet de décentraliser les flux et de garantir une transparence hyaline au public. En outre, elle peut être présentée comme un registre public, infalsifiable, dans lequel tout le monde peut écrire et où chacun peut vérifier le contenu. De ce fait, la notion de « Big Data » est intrinsèquement liée à la blockchain. Nous pouvons définir la « Big Data » par un ensemble de données, provenant de sources diverses (objets connectés, base de données). Ces données peuvent être personnelles (données personnelles, bancaires). Ainsi, elles doivent être protégées, soit par la mise en place d'un système d'anonymisation et de contrôle d'intégrité, soit par un système de chiffrement. L'utilisation des cryptomonnaies, et *in fine*, de la blockchain, favorise la protection et l'anonymat des données, puisqu'elles sont cryptées et ne transitent pas par une autorité centrale. Par ailleurs, les cryptomonnaies n'ont pas besoin des transactions bancaires qui nécessitent toujours une validation de la part d'une ou de plusieurs banques. Ainsi, les données des usagers demeurent décentralisées, anonymes et sécurisées.

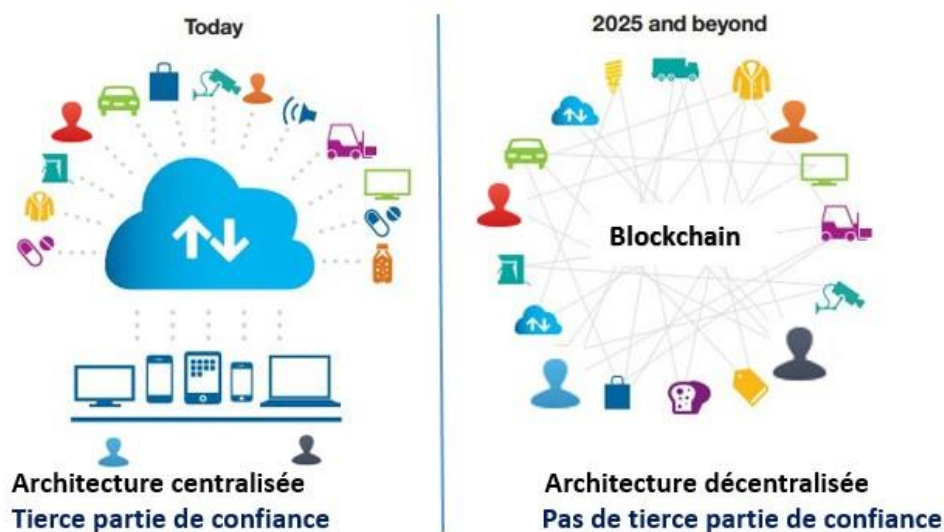
³⁸ Pourquoi les Etats vont lancer leurs propres cryptomonnaies, coinmunity, 12 décembre 2018

³⁹ Les bénéfices sur le bitcoin non taxés au Royaume Uni, Coin24, 01 janvier 2018

⁴⁰ Sputnik News , « « Britcoin » ? Le Royaume-Uni entend se doter d'une crypto-monnaie », 31 décembre 2017

⁴¹ Sputnik News, « « Britcoin » ? Le Royaume-Uni entend se doter d'une crypto-monnaie », 31 décembre 2017

Le système de la blockchain à l'horizon 2025



Source : Blog Big data & Digital, 17 Mai 2016.

Par conséquent, les cryptomonnaies présentent des avantages sécuritaires, le principe de la blockchain rendent la cryptomonnaie infalsifiable rendant les tentatives de fraude extrêmement complexes. Les personnes qui souhaiteraient frauder la blockchain, devront détenir 51% du système (*Attaque des 51%*⁴²). Frauder une monnaie telle que le bitcoin serait tout bonnement impossible puisqu'il faudrait 1 milliard de dollars de matériels et 500 000 euros par heure en électricité.

Nonobstant, certaines dérives des cryptomonnaies pourraient pousser les usagers et le Royaume-Uni à la méfiance. Tout d'abord, certains dénoncent le manque d'anonymat à l'achat des cryptomonnaies. En effet, afin d'acheter de la cryptomonnaie, il est nécessaire de passer par des plates-formes (Marketplace/Cryptoplace) ; la plupart de ces plates-formes exigent une pièce d'identité afin de lutter contre le blanchiment d'argent, en anglais le *money laundering* (AML). Le Royaume-Uni étant membre du groupe d'action financière (GFI créé par le G7 chargé de lutter contre le blanchiment d'argent), les citoyens britanniques sont contraints de « révéler » leurs identités lors de l'achat de cryptomonnaies. Dès lors, l'anonymat n'est plus garanti, tout en sachant que ces plates-formes sont vulnérables. En effet, les cyberattaques contre ces différentes plates-formes sont légion. A titre d'exemple, en juin 2018, deux plates-formes sud-coréennes, Coinrail et Bithumb ont perdu l'équivalent de 46 millions d'euros en cryptomonnaie. En février 2018, une cyberattaque a causé 170 millions d'euros de perte à la plate-forme italienne BitGrail.⁴³

⁴² 18 millions de \$ ont été dérobés sur une blockchain par une attaque des 51. La valeur du Bitcoin Gold a chuté de 20% à l'annonce de cette attaque.

⁴³DURAN Zoe, Les attaques contre les plates-formes de cryptomonnaies se multiplient, AGEFI, 21 septembre 2018

De plus, les processeurs de paiement Bitcoin, à l'instar du géant américain Bitpay, visent à faciliter les transactions mais exigent à ses utilisateurs leurs données personnelles. De ce fait pouvons-nous réellement parler d'anonymat ? Non seulement il y a un partage de données personnelles -de clés publiques- mais cela permet également à l'entreprise de retracer l'ensemble des transactions.

Les États, quant à eux, sont méfiants vis-à-vis de certaines cryptomonnaies étrangères, qui pourraient être utilisées dans une logique de guerre économique (aspiration de données, préparation d'éventuels terrains propices aux cyberattaques, accapuration d'un marché national). Ainsi, des États, à l'instar de la Russie, ont interdit l'achat et la vente de certaines cryptomonnaies sur leur territoire.⁴⁴ Aujourd'hui, il existe des milliers de cryptomonnaies. Certains États, dont le Royaume-Uni, ont bien saisi l'importance stratégiques de ces monnaies. Ils savent pertinemment qu'en étant derrière la création de leurs propres cryptomonnaies, ils pourront en avoir le contrôle et détenir les données qui y transitent - chaque blockchain- est unique, et le protocole qui la régit découle de ses pères fondateurs.

Cette situation incite le Royaume-Uni à devenir un leader mondial sur le marché des cryptomonnaies. L'intérêt des investisseurs britanniques pour le bitcoin et autres devises numériques a explosé après la hausse des prix de décembre 2017. De plus, les britanniques détiennent trois des plus grandes plates-formes de cryptomonnaie (Bitstamp qui a été le premier à « commercialiser » le Ripple, Coinmama et Cexlo). D'après un rapport réalisé par Big innovation Center, DAG global et Deep KnowLedge Analytics, le Royaume-Uni disposerait des ressources nécessaires pour devenir un leader sur le marché des cryptomonnaies. Plus de 500 millions de livres auraient été investies dans les Fintechs nationales liées au cryptomonnaies en 2017-2018.

Sean Kiernan, directeur général de *DAG Global*, prédit même que l'écart entre l'économie traditionnelle et l'économie crypto britannique « *diminuera et finira par disparaître* » dans les prochaines années. De plus, une récente étude menée par l'Imperial College et la plate-forme britannique d'investissements *eToro* considère les cryptomonnaies comme le futur moyen de paiement britannique.⁴⁵

Par ailleurs, certaines cryptomonnaies ont bien saisi les failles du système bancaires et se proposent d'ores et déjà de les combler. Nous pensons notamment au Ripple. Aussi appelé le Ripple Transaction Protocol (RTXP) ou protocole Ripple, il est à l'antipode de la vocation originelle des cryptomonnaies qui sont décentralisées. Le Ripple est une cryptomonnaie centralisée, et son système de la blockchain est géré et centralisé par une seule et unique entreprise. Il vise à faciliter les transactions interbancaires et à remplacer le système SWIFT, qui pour sa part, est désuet et connu pour sa lenteur notoire. L'atout majeur de la start-up américaine est la réduction des délais de transaction : ils passent de plusieurs jours à

⁴⁴ Comptoir national de l'or, « La Russie va lancer sa cryptomonnaie mais pourquoi faire ? », 1^{er} mars 2018

⁴⁵ DURDEN Tyler, « Uk set to become a Blockchain and Crypto economic leader », ZeroHedge, 17 juillet 2018

quelques secondes. Cet atout assurerait une division par deux du coût des opérations bancaires.⁴⁶ De nombreuses banques ont signé des partenariats avec la start-up dont la Bank of England ou bien la banque Santander. Le Ripple révolutionne le secteur bancaire, puisqu'il permet de donner une dimension digitale aux devises. Thierry Dinard, consultant chez HSBC, estime que « *C'est comme si les banques avaient une monnaie unique dont la valeur est universelle* ». ⁴⁷. Selon *The Telegraph*⁴⁸, la Bank of England l'a bien compris et travaille à un projet de cryptomonnaie liée à la livre et placée sous son égide.

Le Swift parvient tant bien que mal à répondre à cette menace en multipliant les innovations dans le secteur bancaire : GPI et *instant payments*. Aussi, afin de se mettre au même niveau que son concurrent, en 2018, Swift a décidé d'expérimenter la blockchain du consortium HyperLedger, mais peine toujours face au Ripple.

Dans un contexte de guerre des données, le Ripple pourrait se présenter au Royaume-Uni comme une alternative au système Swift, teinté par plusieurs affaires liées à l'espionnage américain⁴⁹. En outre, le Ripple pourrait être un des moyens de mieux sécuriser les données et de contourner les *five eyes* ; mais encore faut-il que l'ingérence américaine ne s'y applique pas cette fois-ci.

En somme, le Royaume-Uni a saisi les enjeux stratégiques liés aux cryptomonnaies, mais devra saisir les opportunités qui s'y présentent. L'avènement des *cryptocurrencies* à l'ère de la guerre des data redistribue les cartes, et pousse les différents États à prôner l'utilisation de la blockchain et des moyens de paiement qui en découlent. Mais comment le Royaume-Uni va-t-il tirer son épingle du jeu dans le cadre du Brexit ?

Encadrement légal de la donnée au Royaume-Uni

La législation européenne du RGPD, entrée en vigueur le 25 mai 2018, régissait avant le Brexit la protection des données au Royaume-Uni. Les principes de base du RGPD sont l'uniformisation de la réglementation sur la protection des données au niveau européen, la responsabilisation des entreprises et le renforcement du droit des personnes⁵⁰. Le Royaume-Uni a parallèlement mis en œuvre un mécanisme de protection des données qui dépasse les dispositions énoncées dans la législation européenne : le Data Protection Act (DPA), entré en vigueur le 23 mai 2018. Ce dernier est un ensemble de lois complémentaires qui vise à renforcer la réglementation européenne. Le périmètre de ces législations s'applique également à des sociétés mères situées en dehors du territoire de l'UE. Ainsi, une entreprise extra-européenne ayant une filiale en Europe traitant des données se voit régie par le RGPD même si l'utilisation finale de ces données est effectuée hors de la zone Européenne. Par exemple, l'entreprise « AggregatIQ Data Services Ltd »⁵¹ fût mise en demeure par l'ICO à cause d'un traitement non conforme au RGPD, malgré le fait que la société soit canadienne.

⁴⁶ ROJAS Daxxia, « Ripple veut prendre le relais de SWIFT », AGEFI, 14 novembre 2018

⁴⁷ PERREAU Charlie, « Menacée par Ripple Swift contre-attaque », Journal du net, 24 avril 2018

⁴⁸ MENDICK Robert, Bank of England plots its own bitcoin-style digital currency, 30 décembre 2017

⁴⁹ PERROTIN Maxime, SWIFT – L'Amérique cache ses cartes, Sputnik News, 18 décembre 2015

⁵⁰ ICO, « Investigation into the use of data analytics in political campaigns Investigation update », 11 juillet 2018

⁵¹ FASSINOU Bill, Chroniqueur Actualités, « Le Royaume-Uni a émis la première mise en demeure sous l'ère RGPD », 27 septembre 2018

La donnée personnelle selon la DPA

La définition de la donnée personnelle selon le Data Protection Act correspond à « *toute donnée liée à un individu qui peut être identifié : (a) grâce à cette donnée, ou (b) à partir de cette donnée et d'autres informations qui sont en possession, ou pourrait être en possession du contrôleur de données (data controller)* »⁵².

La protection de données ne s'applique pas aux données des entreprises (personnes morales), le DPA régissant uniquement les données personnelles, et par conséquent les données relatives aux individus. La majorité de ces données personnelles sont stockées sur des serveurs dans des centres de données (*data center*), dont certains sont situés à l'étranger. Le Royaume-Uni est le plus grand marché de centre de données d'Europe ainsi que le troisième au monde⁵³. A titre d'illustration, l'un des data centers de Visa, déservant l'ensemble de l'Europe, est hébergé au Royaume-Uni.⁵⁴

Quels outils pour protéger la donnée ?

L'organisme chargé du respect du RGPD et du DPA est l'Information Commissioner's Office (ICO). Il se voit conférer certains pouvoirs pour enquêter et en appliquer les dispositions du RGPD et du DPA. En effet, l'ICO peut imposer des amendes administratives aux responsables du traitement des données et aux entreprises de traitement pour les plus graves infractions à la loi. L'amende est susceptible de s'élever jusqu'à 4% du CA de l'entreprise. Il est aussi capable d'engager des poursuites pénales si un responsable du traitement des données (ou un sous-traitant) venait à modifier des documents dans l'intention d'empêcher leur divulgation, après une demande d'accès par l'ICO.

Un exemple de l'influence du RGPD dans le secteur bancaire :

Le groupe anglais Gresham se doit de respecter certaines obligations sur le traitement des données clients. Il est tenu de nommer un DPO (Data protect officer) pour le contrôle et le respect des données personnelles. Le groupe est tenu de ne recueillir que les données nécessaires à son fonctionnement et se voit interdire la vente de celles-ci.

Un autre aspect du DPA consiste à assouplir les dispositions légales du RGPD relatives aux droits d'accès et de suppression des données des utilisateurs. L'article 9 de la loi fixe l'âge du consentement au traitement à 13 ans au lieu des 16 ans prescrits par le cadre juridique européen. Il ne s'applique cependant pas aux activités ne relevant pas du droit de l'Union Européenne, telles que celles ayant trait aux questions de sécurité nationale.

⁵² CNRS, « La protection des données au Royaume-Uni », 14 mars 2012

⁵³ Mc CULLAGH Karen , « Brexit: Les conséquences sur la protection des données au Royaume-Uni », 09 mars 2017

⁵⁴ Site officiel Visa « Global transaction processing expande », « Visa possède 4 data centers : deux aux Etats-Unis, l'un au Royaume-Uni et l'un à Singapour », 26 juillet 2017

La RGPD n'offre aux Etats membres de l'Union qu'une marge de manœuvre assez faible en matière de dérogations d'application de la réglementation. Les dérogations nationales peuvent être appliquées uniquement dans les domaines suivants : sécurité nationale, immigration, enquêtes pénales ainsi que pour des raisons de liberté d'expression et d'information (à des fins journalistiques, académiques, artistiques).

Pour cette raison il est important que le RGPD et le DPA 2018 soient mis en relations et lu conjointement. En vertu de l'Investigatory Powers Act⁵⁵ (IPA) du Royaume-Uni, les fournisseurs d'accès internet sont tenus de collecter des historiques de navigation personnels et de les conserver pendant une période pouvant aller jusqu'à 12 mois. Le gouvernement devrait actuellement réviser certaines de ces lois après que des pouvoirs identiques prévus dans l'ancienne législation du "Data Retention and Investigatory Powers Act" (DRIPA) de 2014 aient été jugés illégaux.

Brexit : Quels impacts sur les données personnelles ?

La nouvelle législation Data Protection Act fixe également le cadre permettant au Royaume-Uni de préparer son avenir en dehors de l'Union Européenne. L'absence d'une décision conforme aux normes européennes entraverait le flux de données personnelles provenant des états membres de l'UE. Cela augmenterait le fardeau réglementaire et le coût pour les entreprises établies au Royaume-Uni qui traitent les données personnelles des citoyens de l'UE. Par ailleurs, l'absence d'une équivalence de protection des données entraverait les échanges transfrontaliers de données personnelles. Cela pourrait causer la délocalisation de multinationales et les inciterait à reconsidérer de futurs investissements au Royaume-Uni.

⁵⁵ LASSON Sarah, « Le DPA 2018 implémente le RGPD au UK », 17 juin 2018

Chapitre 3 : Des données personnelles en otage : le danger des databrokers et l'influence américaine

Le Royaume-Uni a ainsi mis en place une stratégie nationale aux objectifs doubles. Il s'agit, dans un premier temps, pour la Couronne britannique, de tirer profit des données afin de soutenir ses entreprises. Dans un deuxième temps, dans un contexte de guerre des data, de se protéger des intrusions étrangères par la mise en place d'un arsenal juridique de protection des données. Néanmoins, cette stratégie s'avère insuffisante face aux mastodontes américains.

Databroker : le middle-man de la data

En charge d'acheter et de revendre des données, les databrokers (aussi appelés « courtiers de la donnée ») ont pour objectif de procurer des données à des fins politiques ou commerciales.

Selon un rapport de l'ICO publié en juillet 2018⁵⁶, certains partis politiques britanniques dont un mouvement politique pro-brexit, Leave.EU, auraient acheté des données personnelles à différents databrokers. Par exemple, dans le cadre de la campagne du Brexit, Cambridge Analytica aurait fourni entre 2015 et 2016, des données personnelles à Leave.EU. Selon cette même source, certains databrokers auraient obtenu ces données de manière illégale. En effet, l'accord qui encadrerait le transfert de ces données ne respectait pas la réglementation (refus par les databrokers de communiquer le nom de l'acheteur des données, par exemple). Pour rappel, Cambridge Analytica est une société fondée à Londres en 2013, spécialiste en analyse de données. Il s'agit d'une filiale de SCL Group, qui compte notamment comme client le ministère de la défense anglais et le Pentagone. Cambridge Analytica s'est également fait épingle au Royaume-Uni dans le cadre d'un scandale impliquant Facebook et le parti Républicain des Etats-Unis. En effet, dans le cadre de la campagne présidentielle de 2016, la société a été accusée d'avoir utilisé illégalement les données personnelles de 30 à 70 millions d'utilisateurs.

Par ailleurs, l'ICO a dressé une liste d'entreprises britanniques spécialisées dans le commerce de données. Parmi celles-ci : Experian, Emma's Diary, Data8 et CACI. Experian est une compagnie basée à Londres, spécialiste de l'information, née de la fusion entre CCN Group, TWR Information Systems & Services et Direct Marketing Technologies, toutes trois américaines.

Le cas particulier de cette liste de databrokers présent sur le marché britannique reste CACI. De son nom complet « *Consolidated Analysis Center Incorporated* », cette entreprise spécialiste de la donnée et dont le siège britannique est à Londres, est originellement une entreprise militaire privée américaine créée en 1962, et notamment impliquée dans le scandale d'Abou Ghraib, en Irak, en 2003⁵⁷, sujet toujours en attente d'une décision de justice⁵⁸. Aujourd'hui géant de l'information et de l'IT, cette entreprise n'a que pour seule activité l'étude de la data, et son historique peut laisser douter d'une possible ingérence américaine dans la collecte de donnée au Royaume-Uni.

⁵⁶ ICO, « Investigation into the use of data analytics in political campaigns », 11 Juillet 2018

⁵⁷ Center for Constitutional Rights, « Accountability for Abu Ghraib Torture by Private Military Contractors », 2015

⁵⁸ WEINER Rachel, « A suit over Abu Ghraib getting to 'what actually happened' », The Washington Post, 22 Septembre 2017

Comme cela a été démontré en première partie de notre étude, il convient de souligner la mainmise des Etats-Unis sur le système de paiements au Royaume-Uni. Le contrôle des principaux fournisseurs d'accès de systèmes de paiement par les Etats-Unis leur permet d'avoir un accès direct aux données de paiement des utilisateurs britanniques. Même lorsque l'acteur est britannique, celui-ci ne peut se défaire de l'influence structurelle des Etats-Unis sur le marché. Les données transitant par les acteurs du Royaume-Uni se retrouvent alors, de nouveau, sous le contrôle de l'ami américain.

QR code et ingérence américaine : l'étude du cas Paysafecash

Paysafecash est une solution de paiement créée par Paysafe Group, proposant au consommateur de régler ses achats en ligne à partir d'espèces, grâce à la technologie du QR code. Plus en détails, l'utilisateur est invité à sélectionner « Paysafecash » comme moyen de paiement pour valider son achat. Après renseignement des informations liées à l'achat (nom, prénom, adresse), un QR code contenant les données de la commande est immédiatement généré, et l'utilisateur n'a plus qu'à l'imprimer ou à l'envoyer sur son téléphone portable. Pour procéder au paiement effectif, il ne lui suffit plus qu'à se rendre dans l'un des différents points de vente ou partenaire « Paysafe », où le QR code sera scanné et l'appoint exact du montant de la commande sera demandé pour valider l'achat.

Exemple de Fintech britannique dynamique, PaySafecash a cherché à répondre à une demande qui s'est accrue les mois suivants le Brexit : une tendance au retour des espèces⁵⁹ qui vient en rupture avec l'appétence britannique pour l'utilisation de la carte de paiement et du sans contact.⁶⁰ Il s'agirait d'un moyen de paiement plus sécurisé que les autres puisque l'utilisateur n'a pas besoin d'enregistrer ses coordonnées bancaires. Cependant, Paysafecash est détenue par Paysafe Group, une holding britannique installée sur l'île de Man (régulée par la FCA). En août 2017, Paysafe Group est racheté pour la somme de 3 milliards de livres par Blackstone⁶¹, une banque d'investissement américaine basée à New-York, et CVC Capital Partners⁶², un fond de capital-investissement localisé au Luxembourg. Cette acquisition a un impact important sur l'accès aux données qui transitent par PaySafecash : en effet, les propriétaires de la donnée sont la société mère et le pays hébergeur des serveurs. Dans ce cas concret, si les QR code permettent de faire remonter des flux de données directement à Paysafecash (nom, prénom, adresse, habitudes de consommation), il est possible de certifier que les détenteurs finaux sont Blackstone et CVC Capital Partners.

⁵⁹ Malgré une sécurité de plus en plus augmentée et une tradition britannique pour le paiement en espèce, l'utilisation de ce moyen de paiement est en constante baisse depuis les années 2000. Selon une étude menée par UK Finance en 2017, l'espèce représentait 62% des transaction, contre 40% en 2016, et une prévision de 21% en 2026. Voir : UK Finance, « UK Cash & Cash Machines », 2017.

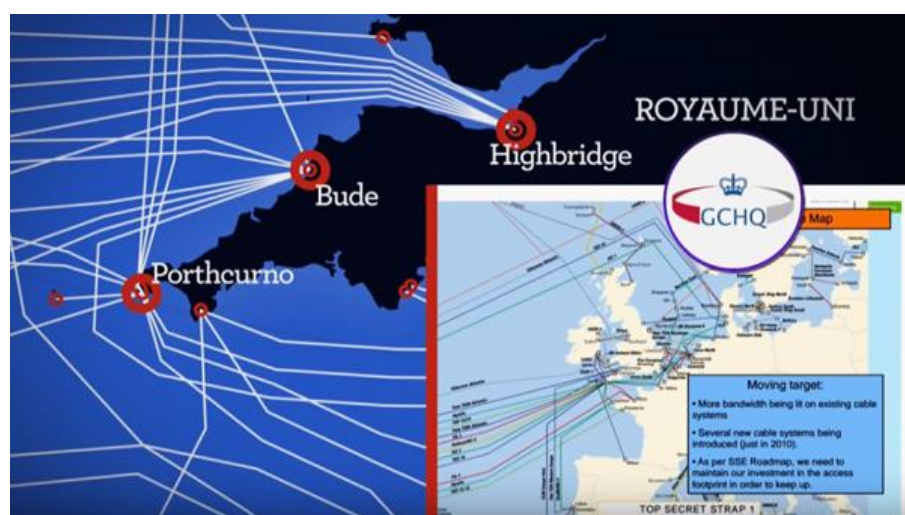
⁶⁰ Selon un communiqué de presse de Paysafe Group⁶⁰, la Bank of England dénombrerait en 2018 2,7 millions de personnes dépendantes de l'espèce, contre 500.000 deux ans auparavant. Voir : Paysafe, Communiqué de presse « Paysafe launches Paysafecash – the ground-breaking new payment solution for the 'cash consumer' », 4 Juin 2018.

⁶¹ S&P Capital HQ, Annexe 11 : fiche d'identité Blackstone,

⁶² S&P Capital HQ, Annexe 12 : fiche d'identité CVC Capital Partners

Ce contrôle de fait du système de paiement britannique par les Etats-Unis est renforcé par l'appartenance du Royaume-Uni aux « *Five Eyes* », l'alliance des services de renseignement des Etats-Unis et du Royaume-Uni, et qui s'est par la suite élargie à l'Australie, à la Nouvelle Zélande et au Canada. Formalisée en 1946 par le *British-U.S. Communication Intelligence Agreement*, l'alliance entre les deux pays se base sur l'échange, par défaut, de tous les renseignements d'origine électromagnétique collectés. La nature et l'étendue du partage d'informations entre les cinq pays demeurent aujourd'hui floues, le dernier document rendu public régissant leurs échanges d'informations datant de 1956.⁶³ Par conséquent, il est difficile d'affirmer que les services de renseignement britanniques respectent les dispositions de la DPA, les obligeant à respecter les normes de protections de données internationales, tant celles-ci sont anciennes. Certains éléments parus dans la presse permettent néanmoins d'apporter des éléments de réponse. Si l'étroitesse des liens entre le Royaume-Uni et les Etats-Unis, alliés de longue date, n'est plus à démontrer, il demeure utile de rappeler que les services de renseignement américains ont financé la remise à niveau des locaux du GCHQ à hauteur de 15.5 millions de livres en 2013.⁶⁴ Il a, en outre, été révélé que les données qui transitent par les câbles sous-marins du Royaume-Uni sont interceptées par le GCHQ depuis le 21 juin 2013⁶⁵ (programme Tempora) puis rendus accessibles à la NSA⁶⁶.

Les câbles sous-marins hébergés au Royaume-Uni



Source : Le Dessous des cartes, « Câbles sous-marins : la guerre invisible »

⁶³ KIM Scarlet, LEE Diana, LUBIN Asaf, PERLIN Paulina, « Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements », Lawfare, 23 avril 2018

⁶⁴ HOPKINS Nick et BORGER Julian, « Exclusive: NSA pays £100m in secret funding for GCHQ », The Guardian, 1er octobre 2013

⁶⁵ VAUDANO Maxime, « Les câbles sous-marins, clé de voute de la cybersurveillance », Le Monde, 6 septembre 2013

⁶⁶ Privacy International, « Policy Briefing – UK Intelligence Sharing Arrangements, Privacy International », Avril 2018

En 2016, *The Guardian* révélait que les services de renseignement britanniques échangeaient les données personnelles (et parmi celles-ci des données dites « financières ») de leurs concitoyens aux pays membres des « Five Eyes »⁶⁷. Selon le *Investigatory Powers Tribunal* chargé de juger cette affaire, « aucune disposition ne régit les garanties à apporter lors de l'échange de données avec des services de renseignement étrangers »⁶⁸. Par ailleurs, un accord bilatéral d'accès aux données collectées par des entreprises entre les deux pays serait à l'étude depuis 2017. D'après le *Financial Times*, sous couvert de lutte contre le terrorisme, cet accord obligerait les « tech companies », et donc possiblement les Fintechs, basées dans l'un des deux pays à transmettre leurs données aux services de renseignement des Etats-Unis ou du Royaume-Uni.

La prépondérance des GAFAs sur le marché de la donnée

Ces nouvelles entités américaines occupent une place prépondérante sur le marché britannique des systèmes de paiement et captent donc les données des citoyens britanniques. D'une part ils possèdent des parts importantes dans les Fintechs : à hauteur de 13% des investissements de Google Venture⁶⁹. Par ailleurs, ces mêmes acteurs adoptent une transformation stratégique visant à leur indépendance vis-à-vis des acteurs bancaires. Google Wallet, Apple Pay, Android Pay ou Azimo via le messenger de Facebook illustrent cette stratégie d'indépendance qui renforce leur position dominante sur le marché. Au Royaume-Uni, les GAFAs ne sont pas soumis à un strict contrôle de la part des autorités britanniques ni à une régulation contraignante comparé aux acteurs bancaires classiques.

De plus, les banques anglaises ont offert à leurs utilisateurs la possibilité de connecter leurs cartes bancaires à Apple Pay afin de pouvoir utiliser les terminaux de paiement installés en UK. Depuis juillet 2015, les utilisateurs de Visa ont accès à ce service. En avril 2016, c'est au tour de Barclays de rejoindre le mouvement. HSBC, NatWest, Santander⁷⁰ et bien d'autres banques acceptent ces partenariats avec ces entités américaines. Cette ingérence américaine par le biais des GAFAs dans les banques anglaises se façonne progressivement et permet une captation légale des données bancaires des utilisateurs.

Cette captation des données par les GAFAs permet de conduire officieusement des études de marché poussées. L'utilisateur offre ainsi aux GAFAs la possibilité de prévoir les opportunités de marché selon l'évolution des comportements.

⁶⁷ BOWCOTT Owen, NORTON-TAYLOR Richard, « UK spy agencies have collected bulk personal data since 1990s, files show », *The Guardian*, 21 avril 2016

⁶⁸ BOWCOTT Owen, « UK spy agencies may be circumventing data-sharing law, tribunal told », 17 octobre 2017

⁶⁹ Medici Team, « What Is Google doing in FinTech ? », *Go Medici*, 10 février 2016

⁷⁰ KELION Leo, « Apple Pay : How it will work in the UK ? », *BBC*, 14 juillet 2015

Brexit : La perspective d'une influence accrue des Etats-Unis sur le contrôle des données britanniques ?

L'avenir du SEPA en question

Le SEPA⁷¹ (Single Euro Payments Area) est un aire économique et financière régie par les banques membres du *Conseil européen des paiements*. Créé en 2012 à la demande de la commission européenne, le SEPA permet aux membres de cet accord de réaliser des opérations bancaires de virement et de prélèvement, à la même vitesse et garantissant la même sécurité qu'une opération domestique. Selon un rapport émis par la Communauté Économique Européenne en Mai 2018, trois issues sont possibles pour le Royaume-Uni pour que celui-ci reste membre de la SEPA⁷² :

- Quitter l'Union Européenne et rester dans l'Espace Economique Européen, et que les lois et réglementations britanniques restent alignées sur le cadre juridique de l'UE ;
- Quitter l'Union Européenne et l'Espace Economique Européen, mais mettre en place un accord de libre-échange, entre l'UE et le Royaume-Uni qui permettrait de répondre aux exigences équivalentes aux critères de participation de la SEPA ;
- Quitter l'Union Européenne, l'Espace Economique Européen, et ne pas accepter d'aligner son cadre juridique sur celui de l'UE. Dans ce cas, son éligibilité ne reposerait uniquement sur le champ d'application géographique de la SEPA (sur évaluation de l'European Payment Council).

Selon un spécialiste des moyens de paiement en France, les relations entre les autorités européennes et le Royaume-Uni sont tendues, et une sortie de la SEPA en mars 2019 (date du Brexit) est inéluctable. De plus, le Royaume-Uni possède son propre outil de prélèvement (le CHAPS), et devrait pouvoir se passer de la SEPA. Néanmoins, cette dernière assurait la protection de donnée personnelles de paiement alors que le CHAPS est, quant à lui, totalement dépendant du SWIFT. Selon un deuxième expert, le SWIFT est contrôlé par les autorités américaines. L'abandon du SEPA par le Royaume-Uni renforcerait donc la mainmise des Etats-Unis sur le système de paiements britannique.

Quel accord de partage de données avec l'Union européenne, et quid des Etats-Unis ?

En tant qu'acteur majeur sur le marché de la donnée, le Royaume-Uni est un partenaire clé de l'Union européenne dans le partage de donnée. En effet, les trois quarts des flux transfrontaliers de données du Royaume Uni transitent par l'Union européenne. Ces partages représentent donc un enjeu majeur tant pour l'Union Européenne que pour le Royaume-Uni. A ce titre, le gouvernement britannique a publié un rapport en novembre 2017 qui envisage un modèle de partenariat post-Brexit de partage de données, fondé sur le dit « *principe d'adéquation* ». Le principe d'adéquation permet au Royaume-Uni, dans le cadre du RGPD, à continuer de

⁷¹ European Payment Council, « About SEPA », site officiel, 2018

⁷² European Payment Council « European Payment Council position on Brexit and UK PSPS' participation in SEPA schemes », 24 Mai 2018

transférer des données avec l'Union Européenne. Des pays non-membres de l'UE, comme l'Argentine, Israël ou la Nouvelle-Zélande, bénéficient de ce principe.

Le gouvernement britannique cherche surtout à préserver son rôle majeur dans le mécanisme européenne de transfert de données, notamment par le maintien de l'ICO au sein du processus décisionnel. Ce maintien lui permettrait de continuer à exercer son influence sur l'élaboration des normes européennes sur le partage de données. Cependant, cette proposition contient une zone d'ombre : aucune discussion n'est mentionnée autour des futurs flux de données qui transiteraient entre le Royaume-Uni et les Etats-Unis. Cela représente un danger pour les données européennes transitant via le Royaume-Uni. Sans garde fou et avec le seul aval du Royaume-Uni, les Etats-Unis pourraient ainsi accéder aux données de l'Union européenne.

CONCLUSION

Le Royaume-Uni exprime clairement sa volonté de s'adapter au monde digital à travers une série de mesures, couvrant un éventail complet d'enjeux stratégiques tant au sens de la sécurité nationale que de la compétitivité de ses entreprises.

Les acteurs bancaires britanniques, après avoir amorcé le mouvement de dématérialisation des moyens de paiement, suivent de très près les évolutions en matière de finance grâce à une coopération entre les acteurs publics et privés. Cette entraide permet au gouvernement de doter ses entreprises, et notamment ses Fintechs, d'outils assurant leur compétitivité sur la scène internationale et, par extension, de consolider son statut de puissance économique. New Payments Architecture, Open Banking ou cryptomonnaies, le Royaume-Uni est prêt à refondre son système financier et à libéraliser la collecte, le stockage et l'utilisation des données de paiement. Il s'agit d'être réactif pour s'assurer de jouer un rôle pionnier dans cette course digitale.

Le Royaume-Uni a su répondre aux enjeux juridiques soulevés par le mouvement de libéralisation des données de paiement en apportant des réponses concrètes. Ainsi, celles-ci dépassent le cadre légal européen de protection des données personnelles. En effet, le RGPD ne permet pas de répondre au problème du traitement des données, enjeu majeur ayant émergé en même temps que la digitalisation des données de paiement. La DPA illustre la volonté d'indépendance normative du Royaume-Uni vis-à-vis de l'Europe et réaffirme sa souveraineté juridique. Cet encadrement assure au Royaume-Uni un avenir dénué de vide juridique en termes de traitement de données après le Brexit. Il s'agit, en somme, d'une prise de conscience nationale sur l'importance stratégique de la donnée. Toutefois, cet encadrement juridique nécessaire n'efface pas les risques en matière de cybersécurité, qui pèsent toujours sur les données de paiement britanniques.

Il convient par ailleurs, de s'interroger sur les liens étroits entretenus entre le Royaume-Uni et les Etats-Unis sur de nombreux plans. En effet, ils ont conduit à l'emprise, par les Etats-Unis, des données qui transitent par le système des paiements du Royaume-Uni. Cette emprise s'exerce par le biais de divers canaux : les fournisseurs d'infrastructures comme Vocalink qu'il est impossible de contourner, les prestataires de services qui sont majoritairement américains, ou encore le rôle prépondérant des GAFAs dans l'ensemble de la structure des paiements. Les accords signés entre les deux pays en matière de renseignement ne fait que renforcer la dépendance du Royaume-Uni vis-à-vis de son allié historique. Cette dépendance de fait n'en est pas moins pleinement consentie. Celle-ci devrait, de plus, s'accroître après la sortie du Royaume-Uni de l'Union européenne. Si pour le moment, cette situation de dépendance semble lui convenir, l'arrivée des nouvelles technologies de plus en plus intrusives concernant les données personnelles, telles que la biométrie, pourraient pousser les britanniques à faire preuve de plus de méfiance (et de discernement ?).

II. GLOSSAIRE

- **Espèce** : Somme d'argent liquide (billets de banques et pièces de monnaies) par opposition à tout autre mode de paiement (chèque, paiement en nature, etc.).
- **Chèque** : Monnaie scripturale permettant le transfert d'un compte bancaire à un autre.

- **Cartes**

- A. Typologie**

- Carte débit : Carte délivrée par un établissement de crédit permettant, entre autres, d'effectuer des paiements auprès des commerçants et dont l'utilisation est adossée à un crédit renouvelable.
- Carte crédit : Carte en plastique comportant une bande magnétique ou une puce intégrée et servant à débiter directement d'un compte courant le prix d'un bien ou d'un service au moment de l'achat.
- Cartes prépayées : Moyen de paiement dont le fonctionnement normal se limite à l'utilisation des fonds chargés par avance.
- Carte points fidélité : permet d'identifier les clients les plus fidèles et de leur attribuer des avantages sous forme de services, cadeaux ou de remises.

- B. Technologie :**

- A bande : Créée en 1971, la carte à bande magnétique est une carte comportant une bande noire à son verso. La bande magnétique sur les cartes de crédits permet donc d'écrire et de lire diverses données comme des noms, des numéros, etc.
- A puce : Une carte à puce est une carte en matière plastique, portant au moins un circuit intégré capable de contenir de l'information.
- NFC (sans contact) : La Near Field Communication, soit Communication en champ proche est une technique de télécommunication par radio à très courte distance, typiquement quelques centimètres (inférieur à 4cm)
- RFID : Le Radio Frequency Identification est une méthode utilisée pour stocker et récupérer des données à distance en utilisant des balises métalliques, les « Tag RFID ». Ces balises, qui peuvent être collées ou incorporées dans des produits, et qui sont composées d'une antenne et d'une puce électronique, réagissent aux ondes radio et transmettent des informations à distance.

● Transferts

- SWIFT : il s'agit d'un acronyme de Society for Worldwide Interbank Financial Telecommunication. Il correspond à un identifiant bancaire normalisé au niveau international pour effectuer des **virements** grâce à l'utilisation unique d'un code attribué à chaque paiement international.
- SEPA : signifie Single Euro Payments Area et désigne l'espace unique de paiements en euro. C'est un projet qui vise à créer un marché européen intégré des paiements pour les organisations et les particuliers qui effectuent ou reçoivent des paiements en euros
- TIP : Il s'agit du virement, du prélèvement automatique et du titre interbancaire de paiement (TIP). Ils sont simples d'usage et très pratiques pour le règlement à distance, notamment de sommes importantes ou pour des règlements réguliers.

● Nouvelles technologies

- QR-code : La technologie QR code, initialement créée au Japon, repose sur l'encodage de différents types de données à l'intérieur d'un code-barres 2D (encodage en largeur et en longueur, contrairement à un simple encodage en longueur pour un code-barres classique). Il en existe différentes versions, permettant de stocker plus ou moins de données.
- M-Banking : Le canal par le biais duquel le client interagit avec une banque via un dispositif mobile pour effectuer des paiements ou utiliser d'autres services financiers mobiles avec une indépendance de temps et de lieu
- Cryptomonnaie : Une cryptomonnaie, dite aussi cryptoactif, cryptodevise ou monnaie cryptographique, est une monnaie utilisable sur un réseau informatique décentralisé, de pair à pair. Elle est fondée sur les principes de la cryptographie et intègre l'utilisateur dans les processus d'émission et de règlement des transactions.
- Via Mobile : Paiement effectué depuis un mobile ou en ligne avec un débit sur carte ou sur portefeuille électronique. Ex : paiement réalisé à distance (ex : sites de commerce électronique), paiement de proximité sur une borne, ou transfert de mobile à mobile.

BIBLIOGRAPHIE

SITOGRAFIE :

AMAZON WEB SERVICE, « AWS Case Study: OakNorth Bank », AWS site officiel, 2018

<https://aws.amazon.com/fr/solutions/case-studies/oaknorth/>

ANUSIC Ingrid, « Will 2018 be the year of contactless payments in the US ? », Network Merchants, 14 février 2018, <https://www.nmi.com/blog/will-2018-be-the-year-of-contactless-payments-in-the-us>

ANDERSON Tony, « The future of money : 2019 promises more dramatic changes in banking and payments », Out Law, 15 mai 2018

<https://www.out-law.com/en/articles/2018/may/future-money-2019-changes-banking-payments/>

ANTHONY Sebastian, « What is Open Banking, and is it safe ? », Bankrate UK, 27 mars 2018

<https://www.bankrate.com/uk/open-banking/what-is-open-banking/>

BOUCHE Thomas-Jérôme, « Qu'est-ce qu'un traitement de données ? », DPO expert, 4 septembre 2018

<https://dpoexpert.fr/traitement-de-donnees/>

BOURSEDIRECT, « Le Royaume-Uni dans le flou sur le Brexit à 100 jours de l'échéance », 19 décembre 2018

<https://www.boursedirect.fr/fr/actualites/categorie/economie/le-royaume-uni-dans-le-flou-sur-le-brexit-a-100-jours-de-l-echeance-afp-be29e3946dc73192febb6af7314fcbebc14cabb4?fbclid=IwAR2uzEoj7-cqpbD7f9Z-0UAXgK90e-YIFD-mINCo7-jPzenWMkGiwsxe-yMY>

BIRCH David, « Forget banks, in 2018 you'll pay through Amazon and Facebook », Wired, 2 janvier 2018

<https://www.wired.co.uk/article/banks-data-tech-giants>

BLOCH Valeska, SMITH Gavin, HIGGINS James, HALL Claudia, ORTNER Alex, Australia moves to Open Banking in 2019, Linklaters, 19 novembre 2018

<https://www.linklaters.com/en/insights/blogs/fintechlinks/2018/november/australia-moves-to-open-banking-in-2019>

BOWCOTT Owen, NORTON-TAYLOR Richard, « UK spy agencies have collected bulk personal data since 1990s, files show », The Guardian, 21 avril 2016

<https://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s>

BOWCOTT Owen, « UK spy agencies may be circumventing data-sharing law, tribunal told », 17 octobre 2017

<https://www.theguardian.com/technology/2017/oct/17/uk-spy-agencies-intelligence-mi5-mi6-law-data-sharing-tribunal>

BRACKERT Thorsten, DAB Stefan, « Retail Banks Must Embrace Open Banking or Be Sidelined », BCG, 8 octobre 2018

<https://www.bcg.com/fr-fr/publications/2018/retail-banks-must-embrace-open-banking-sidelined.aspx>

BRODSKY Laura, IP Chris, and LUNDBERG Tobias, « Open banking's next wave: Perspectives from three fintech CEOs », Mc Kinsey, août 2018

<https://www.mckinsey.com/industries/financial-services/our-insights/open-bankings-next-wave-perspectives-from-three-fintech-ceos>

BURKITT Henry, « New payments architecture : the next big innovation in payments », Out Law, 6 juin 2018

<https://www.out-law.com/en/articles/2018/june/new-payments-architecture-innovation-in-payments/>

CANARDCOINCOIN, « Les bénéficiaires sur le bitcoin non taxés au Royaume Uni », 23 janvier 2018

<http://coincommunity.fr/etats-lancer-propre-crypto-monnaie/>

CAVAGLIERI Chiara, « Open banking : sharing your financial data », Which, octobre 2018

<https://www.which.co.uk/money/banking/switching-your-bank/open-banking-sharing-your-financial-data-anscq4g8p62h>

CLARK Sarah, « Visa targets open banking with \$100m investment fund », NFC World, 5 juin 2018

<https://www.nfcworld.com/2018/06/05/357210/visa-targets-open-banking-with-100m-investment-fund/>

CLELAND Victoria, « La Banque d'Angleterre se prononce sur le renouvellement du système de règlement brut en temps réel (RBTR) et sur les répercussions de la norme ISO 20022 », Paiements Canada, 2018

<https://www.paiements.ca/%C3%A0-propos/nouvelles/la-banque-d%E2%80%99angleterre-se-prononce-sur-le-renouvellement-du-syst%C3%A8me-de-r%C3%A8glement>

CNIL, « La protection des données au Royaume-Uni », Cnil CNRS, 14 mai 2012

<http://www.cil.cnrs.fr/CIL/spip.php?article1532>

COMPTOIR NATIONAL DE L'OR, « La Russie va lancer sa cryptomonnaie mais pourquoi faire ? », 01 Mars 2018

<https://www.gold.fr/news/2018/03/01/la-russie-va-lancer-sa-cryptomonnaie-mais-pour-quoi-faire/>

COUNIS Alexandre, « British Airways victime d'un vaste piratage informatique », Les Echos, 6 septembre 2018

https://www.lesechos.fr/06/09/2018/lesechos.fr/0302219535016_british-airways-victime-d-un-vaste-piratage-informatique.htm

COUNIS Alexandre, « Avec l'Open Banking, le Royaume-Uni a ouvert la voie », Les Echos, 30 novembre 2017

https://www.lesechos.fr/30/11/2017/lesechos.fr/030959746643_avec-l-open-banking-le-royaume-uni-a-ouvert-la-voie.htm

CUNY Delphine, « Paiement : la directive DSP2 entre en vigueur, c'est quoi ? », La Tribune, 13 janvier 2018

<https://www.latribune.fr/entreprises-finance/banques-finance/paiement-la-directive-dsp2-entre-en-vigueur-c-est-quoi-764449.html>

DASKAL Jennifer, « A New UK-US Data Sharing Agreement : A Tremendous Opportunity, If Done Right », Just Security, 8 février 2016

<https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/>

DAANGAR Djasra, « Blockchain et Big Data : enjeux stratégiques ? » Blog Big data & Digital. 17 mai 2016

<https://fr.blog.businessdecision.com/bigdata/2016/05/blockchain-big-data-enjeux-strategiques/>

DURAN Zoe, « Les attaques contre les plates-formes de cryptomonnaies se multiplient », AGEFI, 21 septembre 2016

<https://www.agefi.fr/fintech/actualites/quotidien/20180921/attaques-contre-plates-formes-crypto-monnaies-se-256607>

DURDEN Tyler, « UK set to become a Blockchain and Crypto economic leader », ZeroHedge, 07 août 2018

<https://www.zerohedge.com/news/2018-07-17/uk-set-become-blockchain-and-crypto-economy-leader-new-report-says>

MENDICK Robert, « Bank of England plots its own bitcoin-style digital currency », Telegraph, 30 décembre 2017

<https://www.telegraph.co.uk/news/2017/12/30/bank-england-plots-bitcoin-style-digital-currency/>

EUROPEAN PAYMENT COUNCIL, « About SEPA », 2018
<https://www.europeanpaymentscouncil.eu/about-sepa>

EXPERIAN, “Data Protection Act”, 10 novembre 2016

<https://www.edq.com/uk/glossary/data-protection-act/?fbclid=IwAR0QG5vylwVqEhFd3EgPfZpCmma8YAGVXlnm5L7TAMww-zmXbxhcl4P7KTo>

FACTOCOM, “Annexe traitement de données à caractère personnel ou DPA », 25 mai 2018,

https://www.factocom.fr/wp-content/uploads/2018/05/RGPD_FACTOCOM_V2-1.pdf

FRONTIER ECONOMICS, « The UK digital sectors after Brexit », TechUK, 24 Janvier 2017

<https://www.techuk.org/insights/news/item/10086-the-uk-digital-sectors-after-brexit>

GREEN Andy, « Le GDPR, mais sous un autre nom : la nouvelle loi britannique de protection des données », Blog Varonis, 14 novembre 2017

<https://blog.varonis.fr/le-gdpr-mais-sous-un-autre-nom-la-nouvelle-loi-britannique-de-protection-des-donnees/>

HOPKINS Nick, BORGER Julian, « Exclusive: NSA pays £100m in secret funding for GCHQ », The Guardian, 1er octobre 2013

<https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>

KOUTOULAKOU Iliana, « Numérique : Qui collecte nos données ? », Economie Numérique, 1^{er} décembre 2016

<http://blog.economie-numerique.net/2016/12/01/numerique-qui-collecte-nos-donnees/>

INFORMATION COMMISSER’S OFFICE (ICO), “Guide to the General Data Protection Regulation”

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

KELION Leon, « Apple Pay : How I will work in the UK ? », BBC, 14 juillet 2015

<https://www.bbc.com/news/technology-33489066>

KIM Scarlet, LEE Diana, LUBIN Asaf, PERLIN Paulina, « Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements », Lawfare, 23 avril 2018
<https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing>

de LONGEAUX Claire, « Open Banking, une opportunité bien réelle », La Tribune, 9 novembre 2018
<https://marseille.latribune.fr/idees/2018-11-09/open-banking-une-opportunit-e-bien-reelle-797025.html>

Dr MAC CULLAGH Karen, « Brexit : Les conséquences sur la protection des données au Royaume-Uni », Blog Droit Européen, 9 mars 2017
<https://blogdroiteuropeen.com/2017/03/09/brexit-les-consequences-sur-la-protection-des-donnees-au-royaume-uni-karen-mac-cullagh/>

MANTHORPE Rowland, « What is Open Banking and PSD2 ? WIRED explains », Wired, 17 avril 2018
<https://www.wired.co.uk/article/open-banking-cma-psd2-explained>

MANTHORPE Rowland, « To change how you use money, Open Banking must break banks », Wired, 16 octobre 2017
<https://www.wired.co.uk/article/psd2-future-of-banking>

MARTINEZ Dylan, « Royaume-Uni : le plan post-Brexit de la Banque d'Angleterre », RFI, 20 décembre 2017
<http://www.rfi.fr/europe/20171220-royaume-uni-le-plan-post-brexit-banque-angleterre>

MEDICI TEAM, « What Is Google doing in FinTech ? », Go Medici, 10 février 2016
<https://gomedici.com/what-is-google-doing-in-fintech/>

MERCHANT MACHINE, « Online Payment Systems: 11 Easy To Use UK Options For 2018 », 2018
<https://merchantmachine.co.uk/online-payment-systems/>

OPEN BANKING EXPO, « How Open Banking became a catalyst for mergers », 2018
<https://www.openbankingexpo.com/news/how-open-banking-became-a-catalyst-for-mergers/>

OUT LAW, « Interoperable systems and data at the heart of plans to modernise UK payments infrastructure », 31 juillet 2017
<https://www.out-law.com/en/articles/2017/july/interoperable-systems-and-data-at-the-heart-of-plans-to-modernise-uk-payments-infrastructure/>

OUT LAW, « UK regulator considers opening up access to data from payment systems », 2 juillet 2018
<https://www.out-law.com/en/articles/2018/july/access-to-data-payment-systems/>

PAYSAFE, « Paysafe launches Paysafecash – the ground-breaking new payment solution for the ‘cash consumer’ », 4 Juin 2018
<https://www.paysafe.com/paysafegroup/news/detail/paysafe-launches-paysafecash-the-ground-breaking-new-payment-solution-for-the-cash-consumer/>

PERREAU Charlie, « Menacée par Ripple Swift contre-attaque », Journal du net, 24 avril 2018
<https://www.journaldunet.com/economie/finance/1209061-menace-par-ripple-swift-contre-attaque/>

PERROTIN Maxime, « SWIFT – L'Amérique cache ses cartes », Sputnik News, 18 décembre 2015

https://fr.sputniknews.com/points_de_vue/201512181020374258-amerique-informations-paiement-international/

POUY Gregory, " Vie privée, données personnelles et le RGPD expliqués simplement », French Web, 23 mai 2018

<https://www.frenchweb.fr/vie-privee-donnees-personnelles-et-le-rgpd-expliques-simplement/325010>

PROPP Kenneth, « London Calling: Post-Brexit Prospects for a U.S.-U.K. Digital Trade Deal », Lawfare, 10 décembre 2018

<https://www.lawfareblog.com/london-calling-post-brexit-prospects-us-uk-digital-trade-deal>

RAM Aliya, « Adyen shares almost double on debut », Financial Times, 14 juin 2018

<https://www.ft.com/content/19e5b4aa-6f5c-11e8-92d3-6c13e5c92914>

ROJAS Daxxia, « Ripple veut prendre le relais de SWIFT », AGEFI, 14 novembre 2018

<https://www.agefi.fr/fintech/actualites/quotidien/20181114/ripple-veut-prendre-relais-swift-261092>

SPUTNIK NEWS, « « Bitcoin » ? Le Royaume-Uni entend se doter d'une crypto-monnaie », 31 décembre 2017

<https://fr.sputniknews.com/economie/201712311034570479-banque-angleterre-crypto-monnaie/>

SRUBY Gavin, « Does Open Banking mean the end of card payments ? », Finextra, 25 mars 2018

<https://www.finextra.com/blogposting/15179/does-open-banking-mean-the-end-of-card-payments>

SWIRE Peter, HEMMINGGS Justin, « Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act », Lawfare, 13 septembre 2018

<https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act>

TRIPATHI Ajit, « PSD2 and Open Banking : Success is about building an Ecosystem », LinkedIn, 19 novembre 2016

<https://www.linkedin.com/pulse/psd2-open-banking-success-building-ecosystem-ajit-tripathi/>

TROWER Miles, « Open Banking, fintech and the Brexit hokey cokey », Lexology, 13 août 2018

<https://www.lexology.com/library/detail.aspx?g=9ae39822-f450-4558-af06-cb6bdb8e7326>

VAUDANO Maxime, « Les câbles sous-marins, clé de voute de la cybersurveillance », Le Monde, 6 septembre 2013

https://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html

VIRDI Tony, « La directive PSD2 provoquera l'un des plus importants bouleversements du secteur bancaire depuis des décennies », Finyear, 8 juin 2016

https://www.finyear.com/La-directive-PSD2-provoquera-l-un-des-plus-importants-bouleversements-du-secteur-bancaire-depuis-des-decennies_a36367.html

WEINER Rachel, « A suit over Abu Ghraib getting to 'what actually happened' », The Washington Post, 22 Septembre 2017

https://www.washingtonpost.com/local/public-safety/abu-ghraib-contractor-treatment-deplorable-but-not-torture/2017/09/22/4efc16f4-9e3b-11e7-9083-fbdfdf6804c2_story.html?noredirect=on&utm_term=.ac5241f00ebb

WILLIAMS-GRUT Oscar, « It could be easier for Facebook and Google to get into UK banking thanks to new rules starting Saturday », Business Insider France, 13 janvier 2018

<https://www.businessinsider.fr/us/open-banking-will-facebook-google-and-amazon-get-into-finance-2018-1/>

WILLIAMS-GRUT, « Oscar, Britain is getting a cryptocurrency taskforce », Business Insider, 22 Mars 2018

<https://www.businessinsider.fr/us/uk-chancellor-treasury-cryptocurrency-task-force-2018-3>

ZAGHET Camille, « Le Royaume-Uni manque considérablement de préparation contre les cyberattaques », Siecle Digital, 19 novembre 2018

<https://siecledigital.fr/2018/11/19/le-royaume-uni-manque-considerablement-de-preparation-contre-les-cyberattaques/>

ZDNET, « Data Brokers : aux Etats-Unis, votre vie privée est en vente », 12 avril 2013

<https://www.zdnet.fr/actualites/data-brokers-aux-etats-unis-votre-vie-privee-est-en-vente-39789295.htm>

ZIGAH Xolali, « Pourquoi les Etats vont lancer leurs propres cryptomonnaies », Coinmunity, 12 décembre 2018

<http://coinmunity.fr/etats-lancer-propre-crypto-monnaie/>

RAPPORTS

ACCENTURE, « Review of the International Landscape of Innovation in Payments and Insights for UK Payments », 2014

<https://www.fca.org.uk/publication/other/accenture%20innovation%20report.pdf>

ACCENTURE, « Review of the International Landscape of Innovation in Payments and Insights for UK Payments », FCA.org, 2014

<https://www.fca.org.uk/publication/other/psr-innovation-plenary-accenture.pdf>

BANK OF ENGLAND, « Real-Time Gross Settlement (RTGS) Renewal : Enabling the Next Generation of Payments », 27 septembre 2018

<https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/real-time-gross-settlement-rtgs-renewal-enabling-the-next-generation-of-payments.pdf?la=en&hash=49E47B8951F6FD8D24E6307B36EDAFB7D214B4F5>

CABINET OFFICE, National Security and Intelligence, HM Treasury and The Rt Hon Philip Hammond MP, « National Cyber Security Strategy 2016 to 2021 », Gov.uk, 1^{er} novembre 2016

<https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

CARNEY Mark, « New Economy, New Finance, New Bank », BoE, 21 juin 2018

<https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/new-economy-new-finance-new-bank-speech-by-mark-carney.pdf?la=en&hash=F362C661810257FE779E3D5BCA17144EC65E8C63>

CENTER FOR CONSTITUTIONAL RIGHTS, « Accountability for Abu Ghraib Torture by Private Military Contractors », 2015

<https://ccrjustice.org/sites/default/files/attach/2015/02/PMC%20factsheet%20january%202015.pdf>

CENTRE FOR ECONOMICS AND BUSINESS RESEARCH (CEBR), « Mobile Payments to boost UK economy », 5 novembre 2013

<https://cebr.com/reports/mobile-payments-to-boost-uk-economy/>

PAYMENT SYSTEM REGULATOR (PSR), « Contactless Mobile Payment », Juillet 2018, 3.34

https://www.psr.org.uk/sites/default/files/media/PDF/Contactless_mobile_payments_July_2018.pdf

DELOITTE, « Open Banking and PSD2 : How To Flourish In An Uncertain Future », 2018

<https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-open-banking-how-to-flourish-in-an-uncertain-future.pdf>

EUROPEAN PAYMENT COUNCIL, « European Payment Council position on Brexit and UK PSPS' participation in SEPA schemes », 24 Mai 2018

<https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2018-05/EPC084-18%20EPC%20Position%20paper%20on%20Brexit%20v1.0.pdf>

EY, « Landscaping UK Fintech. Commissioned by UK Trade & Investment », 2014

[https://www.ey.com/Publication/vwLUAssets/Landscaping_UK_Fintech/\\$FILE/EY-Landscaping-UK-Fintech.pdf](https://www.ey.com/Publication/vwLUAssets/Landscaping_UK_Fintech/$FILE/EY-Landscaping-UK-Fintech.pdf)

EY, « UK Fintech on the cutting edge, An evaluation of the international FinTech sector », 2016

<https://www.ey.com/Publication/vwLUAssets/EY-UK-FinTech-On-the-cutting-edge/%24FILE/EY-UK-FinTech-On-the-cutting-edge.pdf>

FINANCIAL CONDUCT AUTHORITY, « Payment Systems Regulator : Who we are and what we do », 22 novembre 2016, p.3

<https://www.psr.org.uk/sites/default/files/media/PDF/intro-to-payment-systems-infographic-Sep2016.pdf>

GILLIGAN Danny, « Global Data Wars: Building a Thriving Data Economy for Australia », Reinventure, 2018

<http://reinventure.com.au/wp-content/uploads/2016/10/GlobalDataWarsReportReinventure.pdf>

HM Government, « The exchange and protection of personal data », 24 août 2017.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

HOWELL Dave, « The future of payments », Information Technology Faculty, 2016

<https://www.icaew.com/-/media/corporate/files/technical/information-technology/technology/185-the-future-of-payments.ashx>

INFORMATION COMMISSIONER'S OFFICE, « Investigation into the use of data analytics in political campaigns », 11 Juillet 2018

<https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>

NAHMIAS Laurent, « Les banques britanniques face au resserrement de la contrainte réglementaire », BNP Paribas - Le portail des études économiques, Juin 2016
<https://economic-research.bnpparibas.com/html/fr-FR/banques-britanniques-face-resserrement-contrainte-reglementaire-27/06/2016,28909>

NATIONAL AUDIT OFFICE, « Investigation : WannaCry cyberattack and the NHS », 24 octobre 2017
<https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

OPEN BANKING WORKING GROUP (OBWG), « The Open Banking Standard : Unlocking the Potential of Open Banking to Improve Competition, Efficiency and Stimulate Innovation », 16 février 2016
<https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%20-%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf>

PAYMENTS UK, « Changing Payments Landscape: How 2017 will change the way we pay for goods », Janvier 2017
https://ctmfile.com/assets/ugc/documents/PMK_Payme_UK_changing-payments-landscape.pdf

PAYMENTS STRATEGY FORUM, « NPA Implementation Plan », juillet 2017
<https://implementation.paymentsforum.uk/sites/default/files/NPA%20Implementation%20Plan.pdf>

PAYMENTS STRATEGY FORUM, « A Payments Strategy for the 21st Century: Putting the needs of users first », Novembre 2016, p.16
https://implementation.paymentsforum.uk/sites/default/files/documents/A%20Payments%20Strategy%20for%20the%2021st%20Century%20-%20Putting%20the%20needs%20of%20users%20first_0.pdf

PAYMENTS STRATEGY FORUM, « Payments Transaction Data Sharing and Data : Scope and Governance Oversight », Novembre 2017
https://implementation.paymentsforum.uk/sites/default/files/documents/Payments%20Transaction%20Data%20Sharing%20and%20Data%20Analytics%20Strategic%20Solution%20-%20Scope%20and%20Governance%20Oversight_0.pdf

PAYMENT SYSTEMS REGULATOR (PSR), « Discussion paper: Data in the payments industry, DP18/1 », Juin 2018
<https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf>

PAYSAFE, « Lost in Transaction: Payment Trends 2018. Will consumers get to grips with frictionless? », 2018
https://www.paysafe.com/fileadmin/content/pdf/Lost_in_Transaction_2018_-_Paysafe_-_web_spreads.pdf

PRIVACY INTERNATIONAL, « Policy Briefing – UK Intelligence Sharing Arrangements », Avril 2018
<https://privacyinternational.org/sites/default/files/201804/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf>

PWC, « Open Banking will shape the future of UK retail and commercial banking », 2018
<https://www.pwc.co.uk/industries/banking-capital-markets/insights/open-banking-shapes-future-uk-retail-commercial-banking.html>

SAGEPAY, « 2017 Payment Landscape Report », 2018

images.go.sage.com/Web/SageGlobalInstance/%7B4135721b-5652-40cf-9f8c-2d7516177777%7D_2017-Landscape-Report.pdf

TechUK, UK Finance, Dentons UKMEA LLP, « No interruptions - Options for the future UK-EU Data-sharing relationship », UK Finance, 30 novembre 2017

<https://www.ukfinance.org.uk/no-interruptions-options-for-the-future-uk-eu-data-sharing-relationship/>

UK FINANCE, « UK Cash & Cash Machines », 2017

<https://www.ukfinance.org.uk/wp-content/uploads/2017/08/Summary-UK-CASH-AND-CASH-MACHINES-3.pdf>

UK FINANCE, « UK Payment Market Summary 2018 », 2018

<https://www.ukfinance.org.uk/wp-content/uploads/2018/06/Summary-UK-Payment-Markets-2018-1.pdf>

COMMUNIQUÉS DE PRESSE

INFORMATION COMMISSIONER'S OFFICE (ICO), "The Information Commissioner's response to the House of Commons Justice Committee consultation on the implications of Brexit for the justice system", 10 novembre 2016

<https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1625633/ico-response-implications-of-brexit-consultation-20161110.pdf>

MASTERCARD, « Mastercard unveils solutions to underpin open banking transformation », 5 juin 2018

<https://newsroom.mastercard.com/eu/press-releases/mastercard-unveils-solutions-to-underpin-open-banking-transformation/>

U.S. COMMODITY FUTURES TRADING COMMISSION, « Signature d'un accord de collaboration entre USA et UK sur l'innovation des technologies financières », 19 février 2018

<https://www.cftc.gov/PressRoom/PressReleases/pr7698-18>

VOCALINK, « Vocalink and Bantec to build and run the infrastructure for the UK's faster image-based cheque clearing », 30 mars 2017

<https://www.vocalink.com/media/2600/fastcheque-press-release-290317.pdf>

MULTIMEDIA

DELOITTE UK, « Open banking: The future of open banking – what do you need to know ? », Youtube, 19 juin 2017

<https://www.youtube.com/watch?v=SCPfkoYFR3Y>

NATIONAL CYBER SECURITY CENTRE (NCSC), « Making the UK the safest place to live and work online », août 2018

https://www.ncsc.gov.uk/content/files/ncsc_2018-annual-review.pdf

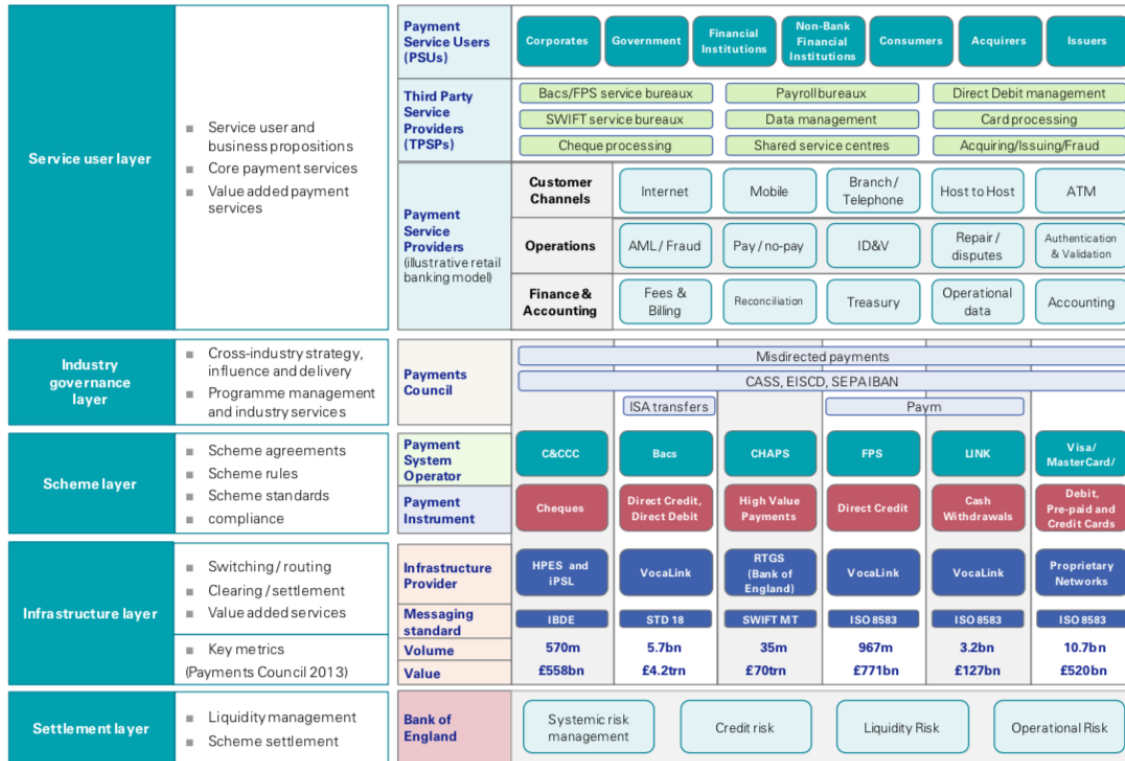
ARTE, « Le Dessous des cartes : Câbles sous-marins la guerre invisible », Youtube, Avril 2018

<https://www.youtube.com/watch?v=RSC0ft-hdRk>

ANNEXES

Annexe 1 : Vue d'ensemble des infrastructures de paiement

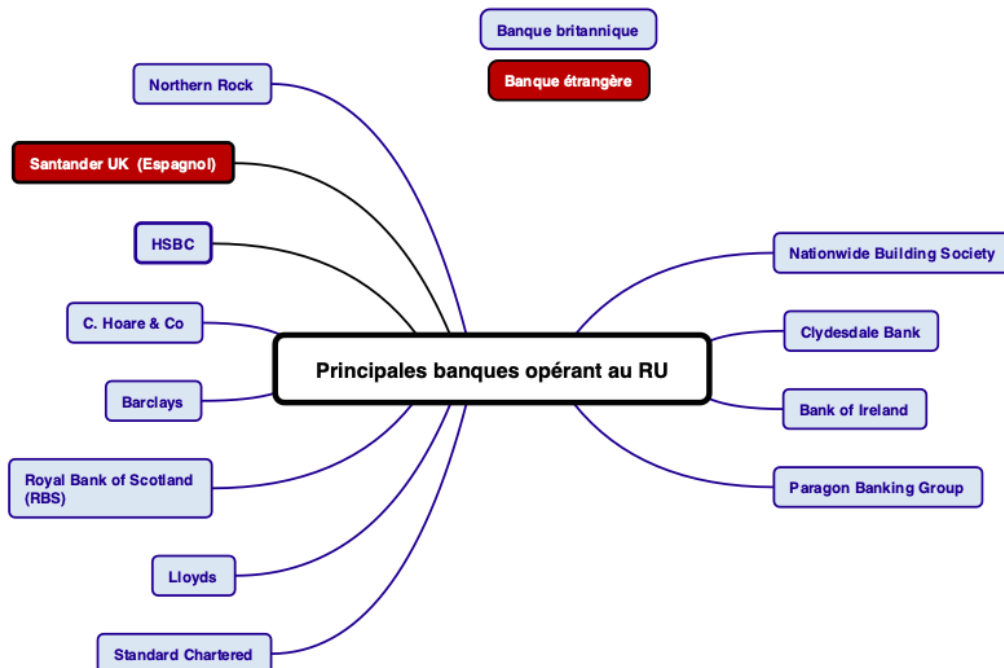
Figure 1: Current UK payments infrastructure overview.



Source : KPMG, UK Payments Infrastructure: Exploring Opportunities, 31 août 2018, p.9
https://www.fca.org.uk/publication/research/kpmg-infrastructure-report-for-psr.pdf?fbclid=IwAR0ZAF-nXagMO5s5beKl7yEN_UtCBL7td9bGAv9_WENotLD6xLV_8YW7m6lg

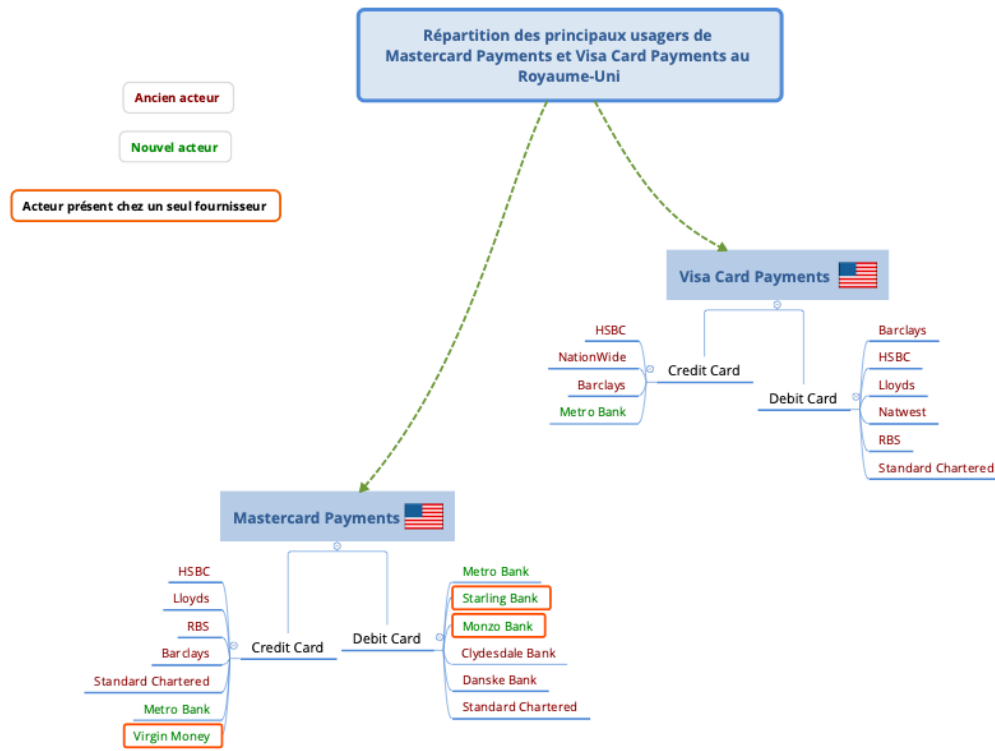
Annexe 2 : Les principales banques opérant au Royaume-Uni

Source : BUCHMULLER T. & DAVID B.



Annexe 3 : Les principaux usagers de Mastercard Payments et Visa Card Payments

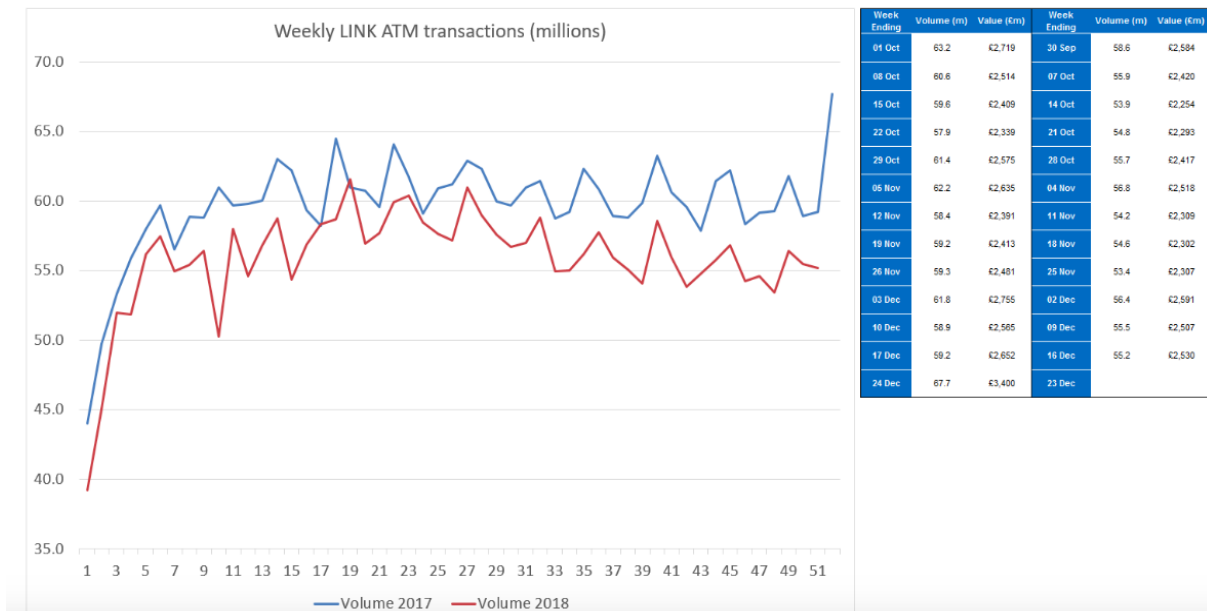
Source : BUCHMULLER T. & DAVID B.



Annexe 4 : Volume et valeur des transactions Link 2017 - 2018

Source : Site officiel Link, 2018

Volume et valeur des transactions LINK par semaine 2017 par rapport à 2018 (en millions)

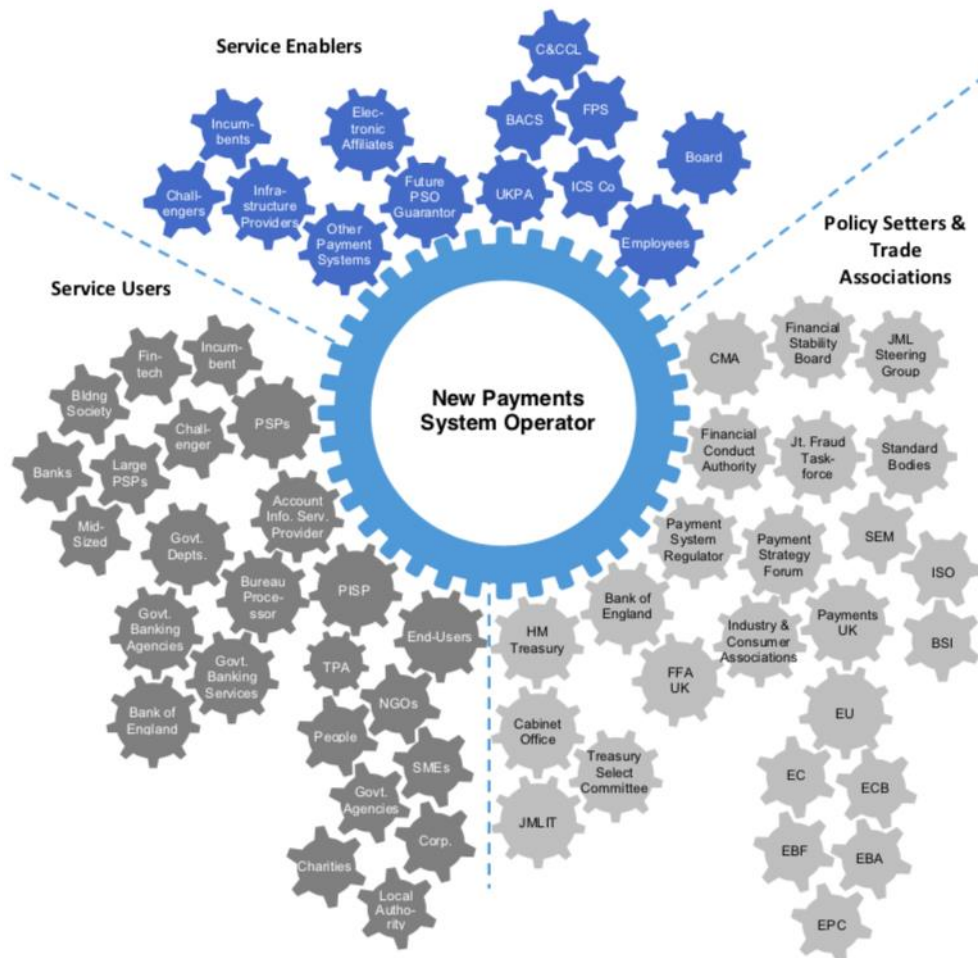


Annexe 5 : Ecosystème du nouvel opérateur de système de paiement au Royaume-Uni

Source : PSO, « Payment System Operator Delivery Group Report », 4 mai 2018, p.53

<https://www.psr.org.uk/sites/default/files/media/PDF/PSODG-Report-2017.pdf>

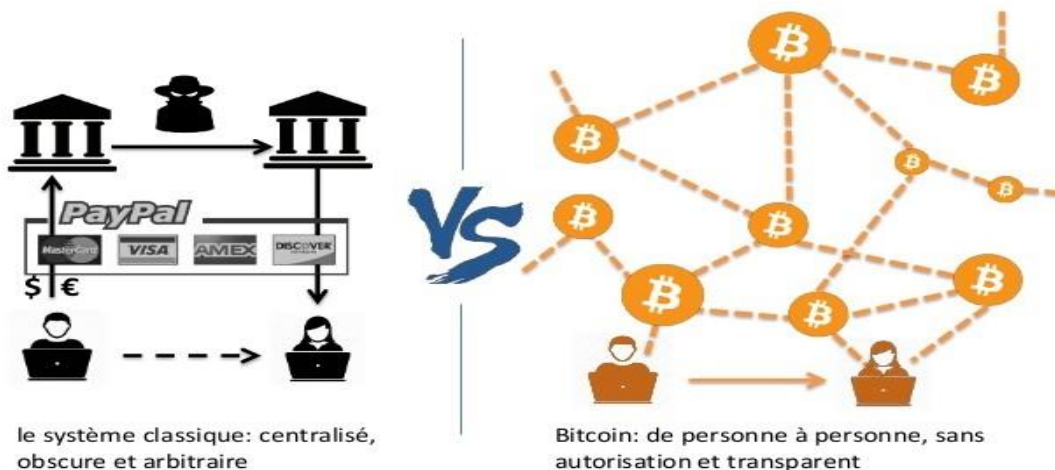
Figure 9. NPSO stakeholder ecosystem



Annexe 6 : Système classique VS Bitcoin

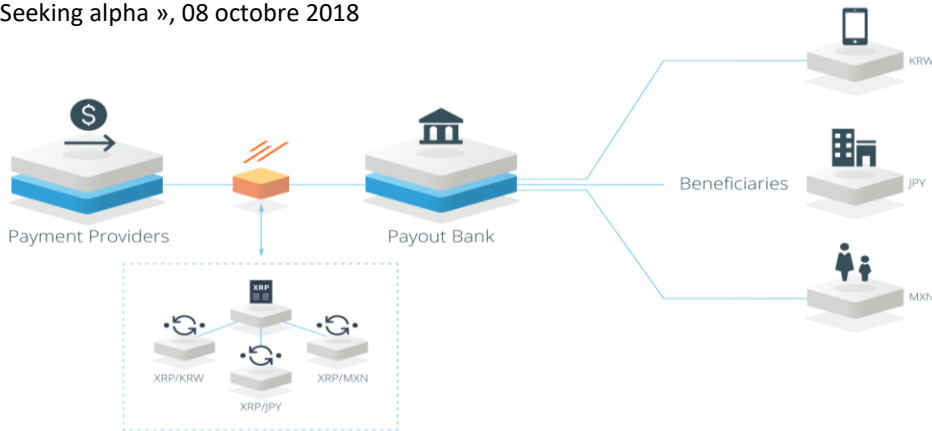
Source : DAANGAR Djasra,, « Blockchain et Big Data : enjeux stratégiques ? » Blog Big data & Digital. 17 mai 2016

<https://fr.blog.businessdecision.com/bigdata/2016/05/blockchain-big-data-enjeux-strategiques/>



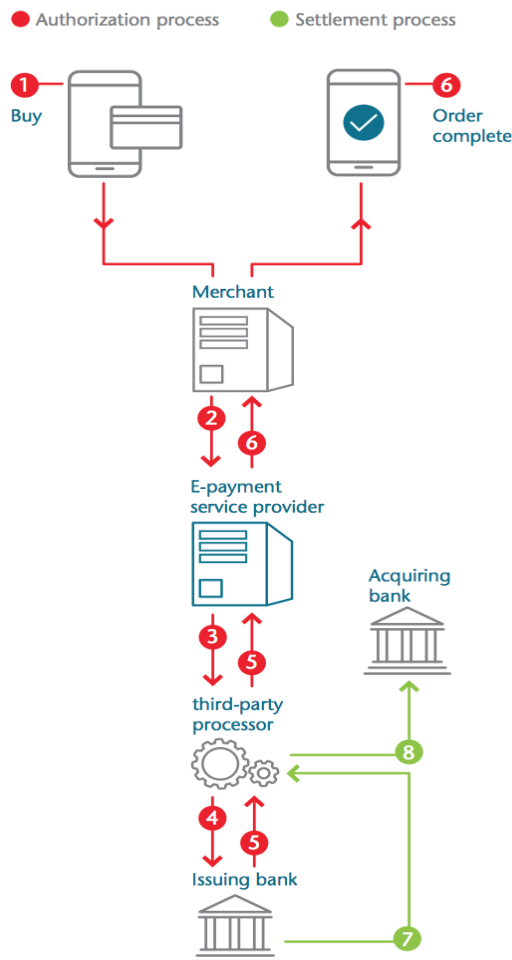
Annexe 7 : Le fonctionnement du Ripple

Source : The freedonia cooperative, « Ripple’s xrapid may save blockchain, but won’t be much for Long-term Investor, Seeking alpha », 08 octobre 2018



Annexe 8 : Le fonctionnement du paiement en ligne

Source : HOWELL Dave, « The future of payments », Information Technology Faculty, 2016, p.5 (Cybersource) <https://www.icaew.com/-/media/corporate/files/technical/information-technology/technology/185-the-future-of-payments.ashx>

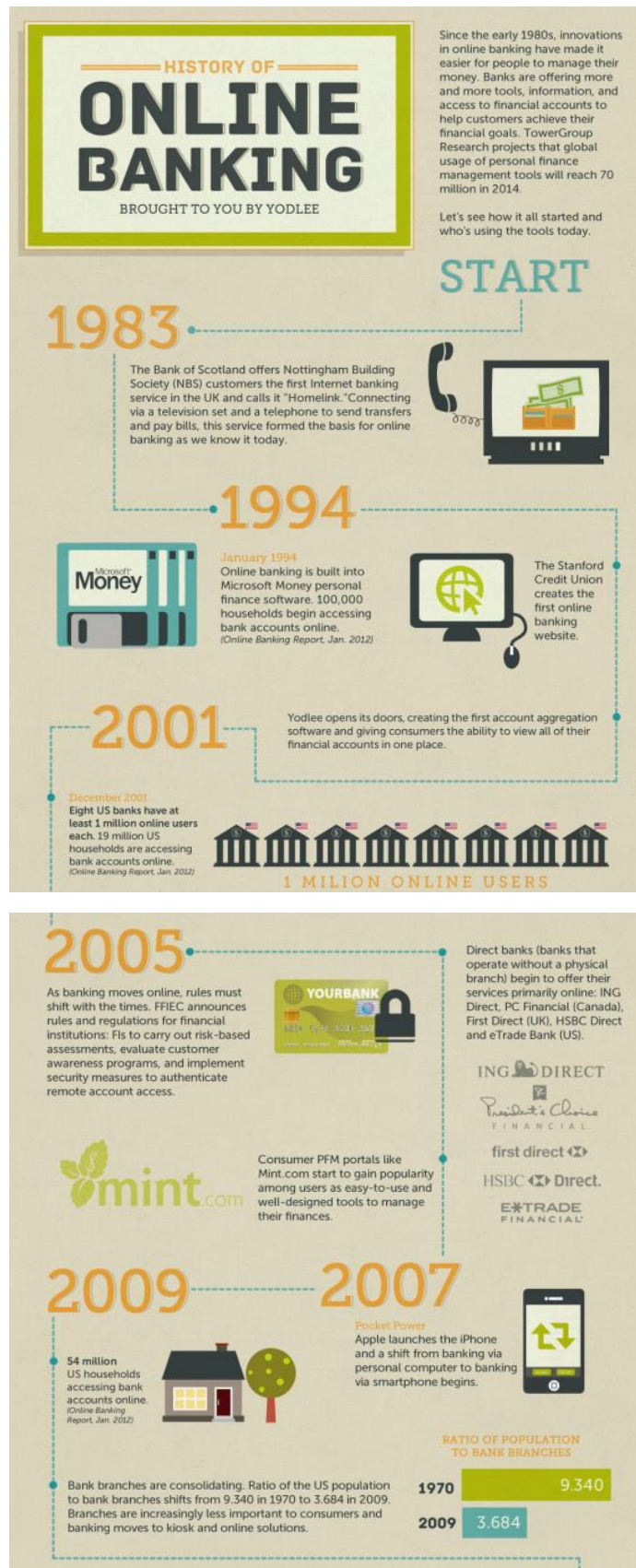


Source: CyberSource

Annexe 9 : La transformation du système bancaire

Source : Jeffry Pilcher, Infographic : The History Of Internet Banking, The Financial Brand, 2 Octobre 2012

<https://thefinancialbrand.com/25380/yodlee-history-of-internet-banking/>



Suite annexe 9



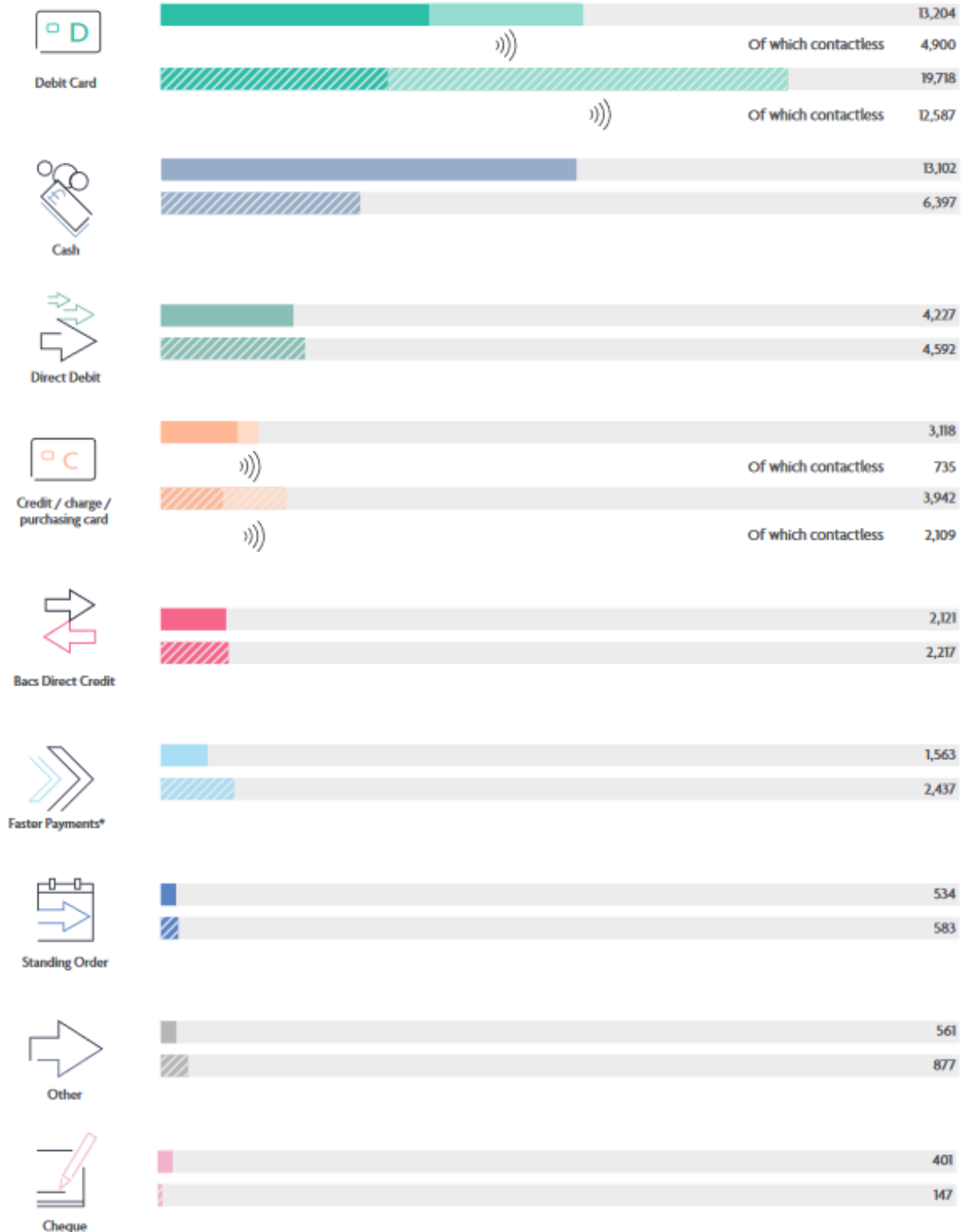
Annexe 10 : Panorama des modes de paiement britanniques en 2017

Source : UK Finance, « UK Payment Market Summary 2018 », 2018, p.9

<https://www.ukfinance.org.uk/wp-content/uploads/2018/06/Summary-UK-Payment-Markets-2018-1.pdf?fbclid=IwAR2YI0DOnJVZVfxk82wivJ5YIMtF9Q5WH1-a-S08U-JyA86WO-CupE3SDQ8>

Payment volumes 2017 v 2027

Total payments (millions) ■ 2017 38,830 ▨ 2027 40,908



*and other remote banking

Annexe 11 : Fiche d'identité de Blackstone

The Blackstone Group L.P. (NYSE:BX)

Year Founded: 1985

S&P Issuer Credit Rating FC LT:
A+

345 Park Avenue
New York, New York 10154
United States
Phone: 212-583-5000
www.blackstone.com

The Blackstone Group L.P. is a publicly owned alternative asset manager. The firm also provides capital markets services to its clients. It provides its services to public and corporate pension funds, academic, cultural, and charitable organizations, retirees, sovereign wealth funds, and institutional and individual investors. The firm manages separate client focused portfolios for its clients. It also launches and manages private equity funds, real estate funds, funds of hedge funds, collateralized loan obligations, real estate investment trusts, and credit-focused funds for its clients. The firm invests in private equity, public equity, fixed income, and alternative investment markets across the globe. The Blackstone Group L.P. was founded in 1985...

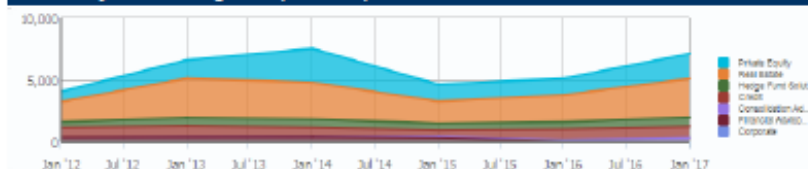
Key Statistics

	12 Months Dec-31-2016A	12 Months Dec-31-2017A	12 Months Sep-30-2018A	12 Months Dec-31-2018E	12 Months Dec-31-2019E
Total Revenue	4,973.18	6,921.57	8,067.58	7,049.52	7,695.86
Growth Over Prior Year	10.5%	39.2%	22.4%	3.9%	9.2%
Gross Profit Margin %	82.5%	78.5%	80.5%	-	-
Net Income Margin %	20.9%	21.2%	23.0%	50.5%	51.8%
Diluted EPS Excl. Extra	1.56	2.21	2.74	2.94	3.22
Diluted EPS Excl. Extra	50.4%	41.4%	20.0%	4.5%	9.6%

Top Holdings (USD)

Company Name	Industry	Shares	% of CSO	Market Value (USD in mm)	% of Portfolio	% Change (Quarter)
Cheniere Energy...	Oil and Gas	203,360,965	58.333	7,587.4	31.46	0.00
Invitation Homes Inc.	Residential REITs	219,945,349	42.250	4,563.9	18.92	0.00
Gates Industrial...	Industrial Machinery	266,873,282	92.086	3,560.1	14.76	9.38
Hispania Activos...	Diversified REITs	98,884,330	90.689	2,056.2	8.52	447.14
Mphasis Limited	IT Consulting and	101,230,853	52.338	1,419.8	5.89	0.00
Hembla AB (publ)	Diversified Real	39,054,257	45.438	659.6	2.73	0.00
The Stars Group Inc.	Casinos and Gaming	24,407,188	8.935	399.6	1.66	-
Vivint Solar, Inc.	Electrical	74,359,374	62.322	329.4	1.37	(9.71)

Revenue by Business Segments (USD, mm)



* Segments with negative values, such as corporate eliminations, are excluded from the total and percentage calculations and do not appear on the charts

Market Data

Last (Delayed)	28.98	Market Cap (mm)	19,007.6
Open	28.79	Implied Market...	34,189.4
Previous Close	28.70	Shares Out. (mm)	662.3
Change on Day	0.28	Implied Shares...	1,191.3
Change % on Day	1.0%	Float %	99.5%
Shares Sold	27.9	Dividend Yield %	9.4%
Day High/Low	29.0/28.5	Diluted EPS Excl....	2.74
52 wk High/Low	40.6/28.6	P/Diluted EPS	10.47x
Volume (mm)	3.30	Avg 3M Dly Vol	6.03
Beta 5Y	1.28		

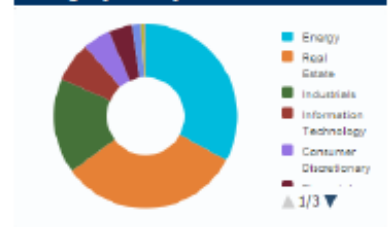
Share Price & Volume (USD)



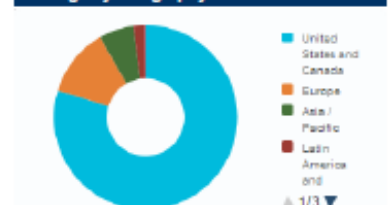
Key Executives and Professionals

Schwarzman, Stephen	Chairman, CEO &...
James, Hamilton	Executive Vice...
Gray, Jonathan D.	President, COO &...
Nash, Michael B.	Sr MD & Co-
Prendergast, Daniel J.	Founder, CEO &...

Holdings by Industry



Holdings by Geography



Capitalization

Share Price as of	28.70
Shares Out.	662.29
Market Capitalization	19,007.64
Book Value of Common	6,987.52
+ Book Value of Pref. Equity	-
= Total Equity	14,706.98
Impl. Shares Out	1,191.27
Impl. Market Cap	34,189.40

Latest Current and Pending Direct Investments

Announced Date	Company Name	Transaction Type	Size (USD in mm)	Transaction Feature	Status	Co-Investors
Dec-10-2011	Portfolio of 55 logistics...	Merger/Acquisition	-	Acquisition of Equity	Current Investment	-
Dec-05-2011	Kryalos Investments Srl	Merger/Acquisition	-	Acquisition of Equity	Pending	-
Dec-01-2011	Seven office buildings	Merger/Acquisition	-	Acquisition of Equity	Current Subsidiary...	-
Nov-15-2011	Cyber Global Risk...	Private Placement	30.00	Venture Capital	Current Investment	Aetna Ventures, LLC, Allegis
Nov-01-2011	Institutional Capital...	Private Placement	-	Venture Capital	Current Investment	JPMP Capital, LLC, The Carlyle

Date Created: Dec-19-2018

Copyright © 2018 S&P Global Market Intelligence, a division of S&P Global Inc. All Rights reserved.

S&P
Capital IQ

Historical Equity Pricing Data supplied by Interactive Data Pricing

and Reference Data LLCs

Credit Default Swaps data provided by ICE CMA

Annexe 12 : Fiche d'identité de CVC Capital Partners

CVC Capital Partners Limited

Year Founded: 1981

Parent Company: CVC Capital Partners Limited

111 Strand
London, Greater London WC2R
0AG
United Kingdom
Phone: 44 20 7420 4200
www.cvc.com

CVC Capital Partners Limited is a private equity firm specializing in middle market, mature, expansion, successions, management buyouts, buyins, leveraged buyouts and buyins, recapitalization, restructuring, growth, growth equity, and acquisitions in Fintech sector. The firm makes investments in medium to large sized companies. It seeks to invest in healthcare, industrial and service sectors including telecommunications, information technology, electronics, biotechnology, medical, energy, chemistry, new materials, industrial automatisms, tech-enabled businesses such as human resources software, data centers, software as a-service, infrastructure, and payments, industrial goods and services, other manufactured goods, financial services, manufacturing...

Top Managed Funds

Fund Name	Equity Assets (USD in mm)	Investment Style
CVC Capital Partners VII, LP	18562.54	Private Equity
CVC European Equity Partners VI LP	14907	Private Equity
CVC European Equity Partners V, L.P.	14253	Private Equity
CVC European Equity Partners IV, L.P.	7278	Private Equity
CVC European Equity Partners Tandem Fund	5618.31	Private Equity
CVC Strategic Opportunities Fund	4500	Private Equity
CVC Capital Partners Asia Pacific III, L.P.	4120	Private Equity
CVC European Equity Partners III	3970	Private Equity
CVC Capital Partners Asia Pacific IV, L.P.	3500	Private Equity
CVC European Equity Partners II LP	3333	Private Equity

Top Holdings (USD)

Company Name	Industry	Shares	% of CSO	Market Value (USD in mm)	% of Portfolio	% Change (Quarter)
Avast Plc	Systems Software	216,303,002	22.687	729.2	-	0.00
Ahlsell AB (publ)	Trading Companies and	109,578,323	25.525	634.9	-	0.00
The Stars Group Inc.	Casinos and Gaming	26,962,108	9.871	441.4	-	-
PT Link Net Tbk	Alternative Carriers	1,017,766,198	33.450	335.0	-	0.00
PT Siloam International	Health Care Facilities	414,797,129	25.514	103.0	-	53.79
Magnum Berhad	Casinos and Gaming	70,000,000	4.919	32.4	-	(56.25)
Lecta SA	Paper Products	316,046	101.625	-	-	0.00

Key Executives and Professionals

Name	Title	Specialty	Fund Affiliations
Van Rappard, Rolly	Co-Founder, Co-Chairman and Managing Partner-Co-	Global	CVC European Equity Partners V, L.P.
Koltes, Steven	Co-Founder & Co-Chairman	-	-
Lucas, Robert R.	Managing Partner, Head of UK Investments &	United Kingdom	CVC European Equity Partners V, L.P.
MacKenzie, Donald	Co-Founder, Co-Chairman, Managing Partner and	Global	CVC European Equity Partners V, L.P.

Limited Partners

Company Name	Investment Value (USD in mm)	Investor Associated Fund
Abbott Capital Management, L.L.C.	-	Abbott Capital Private
Aberdeen Asset Investments Limited	-	Aberdeen Private Equity
Aberdeen Asset Management PLC	-	Aberdeen Private Equity
Aberdeen SVG Private Equity	-	Aberdeen Diamond Private...
Abu Dhabi Investment Company	-	-
ACE & Company SA	-	-
Alameda County Employees' Retirement Association	-	-

Latest Current and Pending Direct Investments

Announced Date	Company Name	Transaction Type	Size (USD in mm)	Transaction Feature	Status	Co-Investors
Dec-11-2018	Ahlsell AB (publ)	Merger/Acquisition	2947.78	Acquisition of Equity	Pending	-
Dec-06-2018	Recordati Industria...	Merger/Acquisition	3088.83	Acquisition of Equity	Pending	CVC Capital Partners VII, LP
Nov-16-2018	DKV MOBILITY	Merger/Acquisition	-	Acquisition of Equity	Pending	CVC Capital Partners VII, LP
Nov-07-2018	Breitling SA	Merger/Acquisition	-	Acquisition of Equity	Current Investment	-
Nov-06-2018	ConvergeOne Holdings,	Merger/Acquisition	1654.61	Acquisition of Equity	Pending	CVC Capital Partners VII, LP

Date Created: Dec-19-2018

Copyright © 2018 S&P Global Market Intelligence, a division of S&P Global Inc. All Rights reserved.

**S&P
Capital IQ**

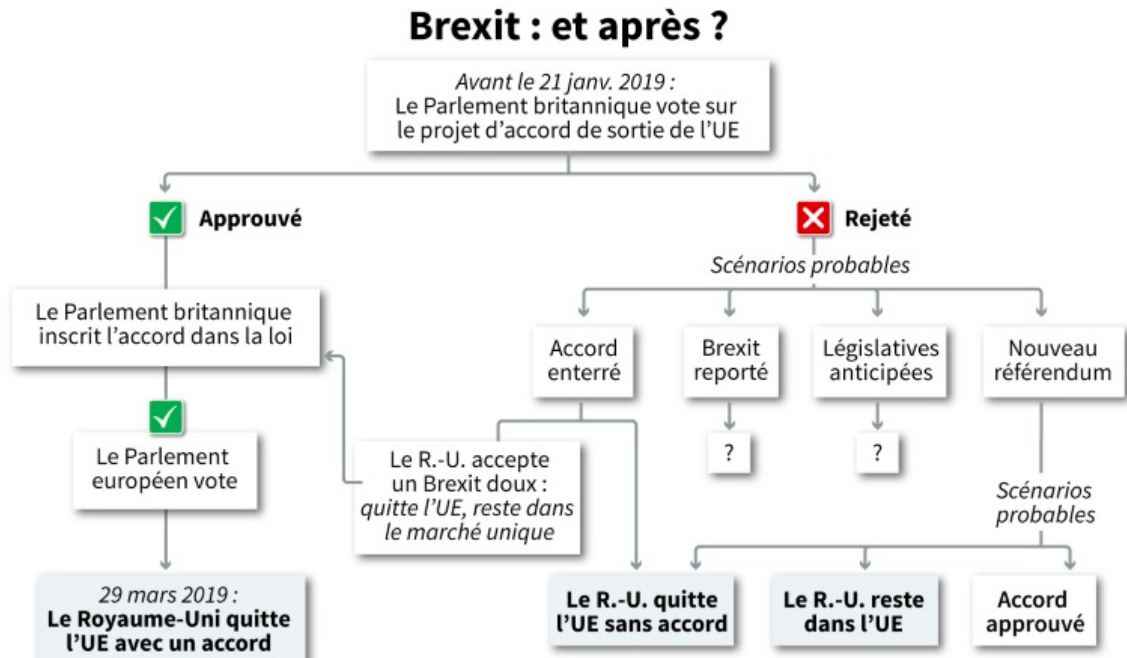
Historical Equity Pricing Data supplied by Interactive Data Pricing

and Reference Data LLCs

Credit Default Swaps data provided by ICE CMA

Annexe 12 : Les options du Brexit

Source : BOURSEDIRECT, « Le Royaume-Uni dans le flou sur le Brexit à 100 jours de l'échéance », 19 décembre 2018 (AFP)



© AFP

Sources : AFP, Chambre des communes, Institute for Government, Open Britain