

# Le numérique et les monnaies

1 Monnaie et dématérialisation

2 Monnaie, numérique et sécurité

3 Vers une guerre des crypto-monnaies ?

# 1 Monnaie et dématérialisation

La monnaie est apparue vers 3 000 avant Jésus-Christ, principalement en Mésopotamie (entre l'Iran et l'Irak).

Son apparition est très liée à l'intensification des échanges : le troc devenait trop compliqué et supposait qu'un acheteur ait en même temps quelque chose à vendre.

Dès le début la monnaie a exigé trois qualités :

- elle doit être un équivalent général, capable d'exprimer la valeur de toutes les choses. Elle doit donc être suffisamment divisible pour exprimer de la plus petite à la plus grande valeur.

- elle doit être un instrument d'échange, ce qui suppose qu'elle ait un pouvoir libératoire : en d'autres termes elle doit être acceptée par tous.

- elle doit être un instrument de réserve permettant un décalage temporel entre un achat et une vente, ce qui suppose que sa valeur soit relativement stable et qu'elle soit inaltérable.

Nous pouvons déjà remarquer que les crypto-monnaies remplissent très difficilement ces conditions : elles ne sont donc pas (encore ?) de vraies monnaies.

Très vite, les hommes ont compris qu'il fallait que la monnaie ait une 4<sup>o</sup> qualité : il faut qu'elle soit suffisamment abondante pour permettre les échanges, donc la production, donc la prospérité.

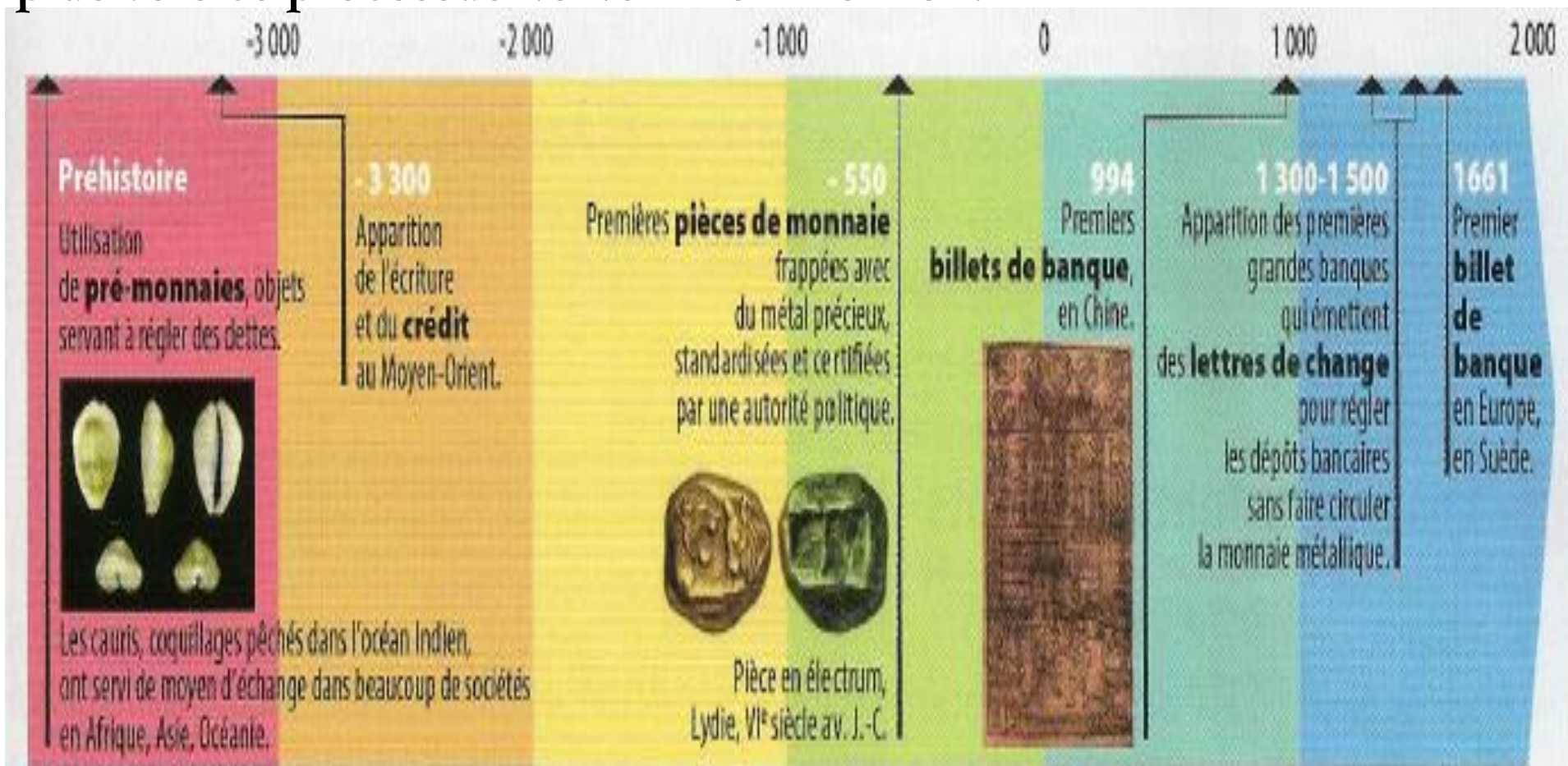
Mais il ne faut pas, néanmoins, qu'elle soit trop abondante pour ne pas perdre de sa valeur, ce que l'on appelle l'inflation.

L'histoire de la monnaie est donc l'histoire de sa dématérialisation : les hommes se sont rendus compte que la monnaie matérielle présentait trois inconvénients :

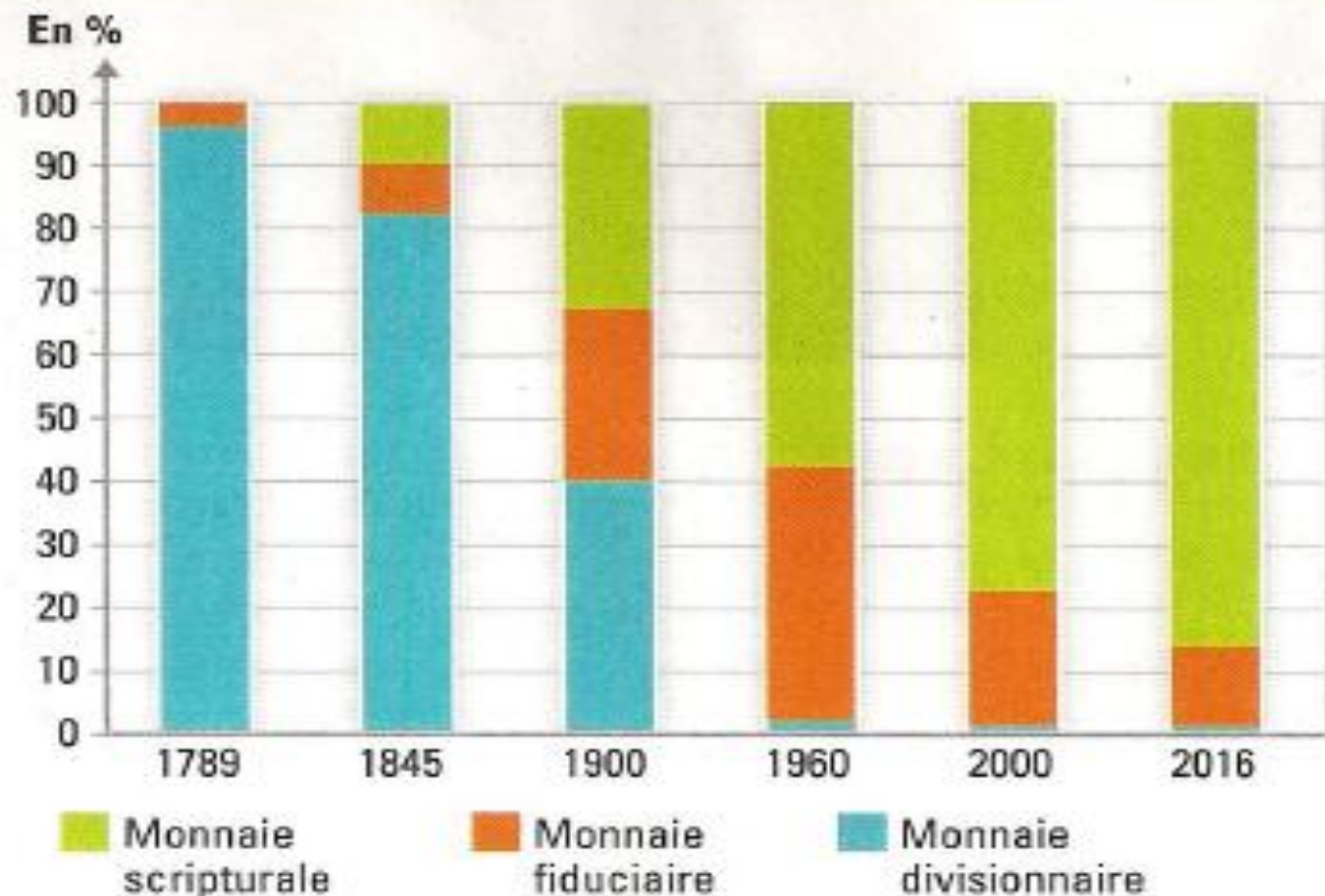
- elle n'est pas pratique, lourde, volumineuse...
- elle peut facilement être dérobée
- surtout, elle est assez rare et entrave les échanges : seules les découvertes d'or et d'argent assuraient cette prospérité, ce qui était trop hasardeux.

Les hommes ont donc souhaité deux choses un peu contradictoires : s'affranchir de la rareté et garantir néanmoins la valeur de la monnaie.

La monnaie sous sa forme numérique n'est donc qu'une étape de plus vers ce processus de dématérialisation.



D'après Citeco, 10 000 ans d'économie.



D'après Jean Bouvier, *Un Siècle de banque française*, Hachette, 1973  
 et Dominique Plihon, *La monnaie et ses mécanismes*,  
 Repères, La Découverte, 2017, données BCE.

L'essentiel de la monnaie aujourd'hui est donc scripturale, et nous ne la voyons jamais : les échanges de monnaie ne se font que par transferts de compte à compte, sous la surveillance des banques centrales.

De ce côté, la monnaie numérique ne va pas changer grand-chose : elle va accélérer un processus déjà largement engagé et elle permettra des échanges de plus en plus rapides et pratiques.

Déjà, dans l'Union européenne comme en France, l'essentiel des paiements se fait par cartes bancaires, par prélèvements ou par virements, c'est à dire sans aucun contact physique avec la monnaie.

L'usage des monnaies reste, on le sait, encore un peu différent selon les pays : si la France est un peu plus utilisatrice des cartes que la moyenne de l'Union européenne (53% des paiements contre 49%), l'Allemagne l'est un peu moins.

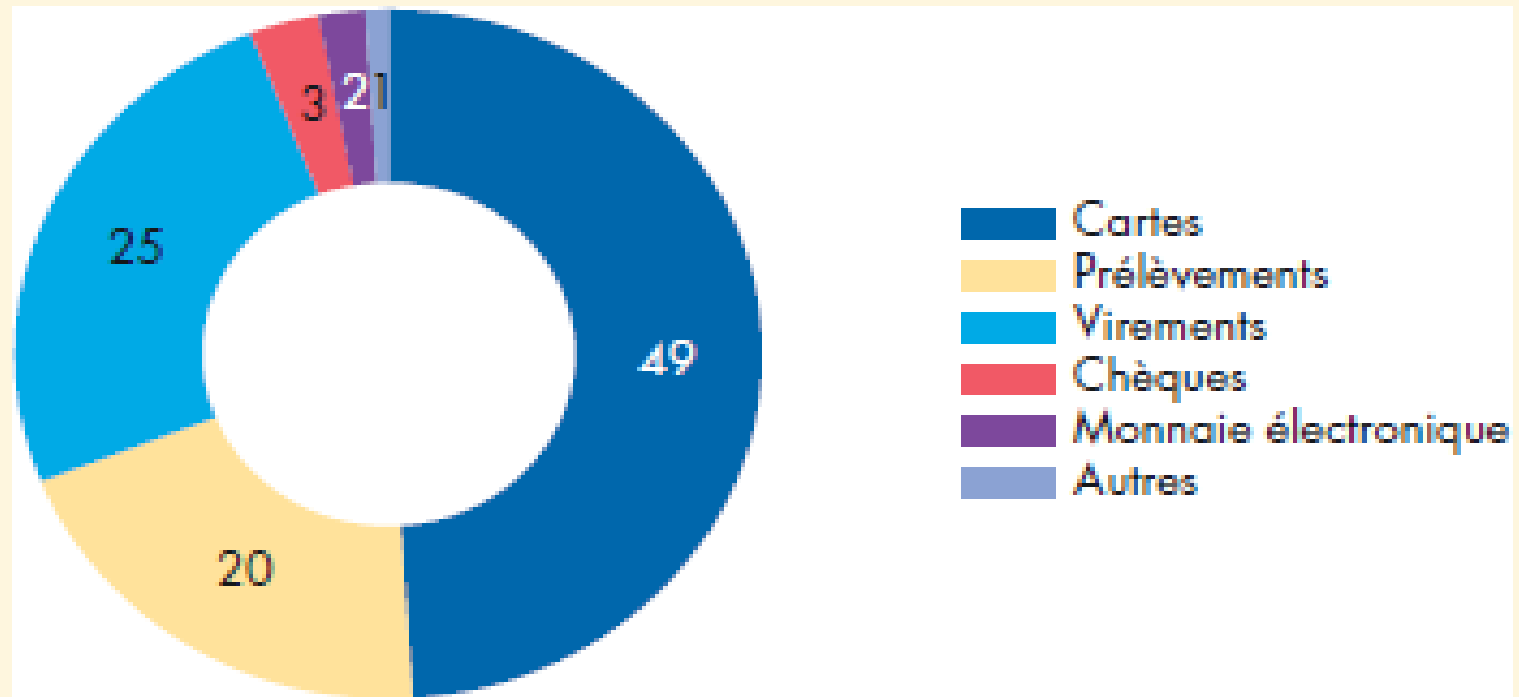
La Suède veut aller encore plus loin et proscrire définitivement la monnaie papier (monnaie fiduciaire) et bien entendu les pièces (monnaie divisionnaire).

Que ce soit dans l'Union européenne ou en France, l'essor du paiement par carte, moyen numérique par excellence, semble irrésistible et définitif.

Mais bientôt, un nouvel enjeu va se dessiner : se passer de carte tout court.

### G3 : Répartition de l'utilisation des différents moyens de paiement scripturaux dans l'Union européenne

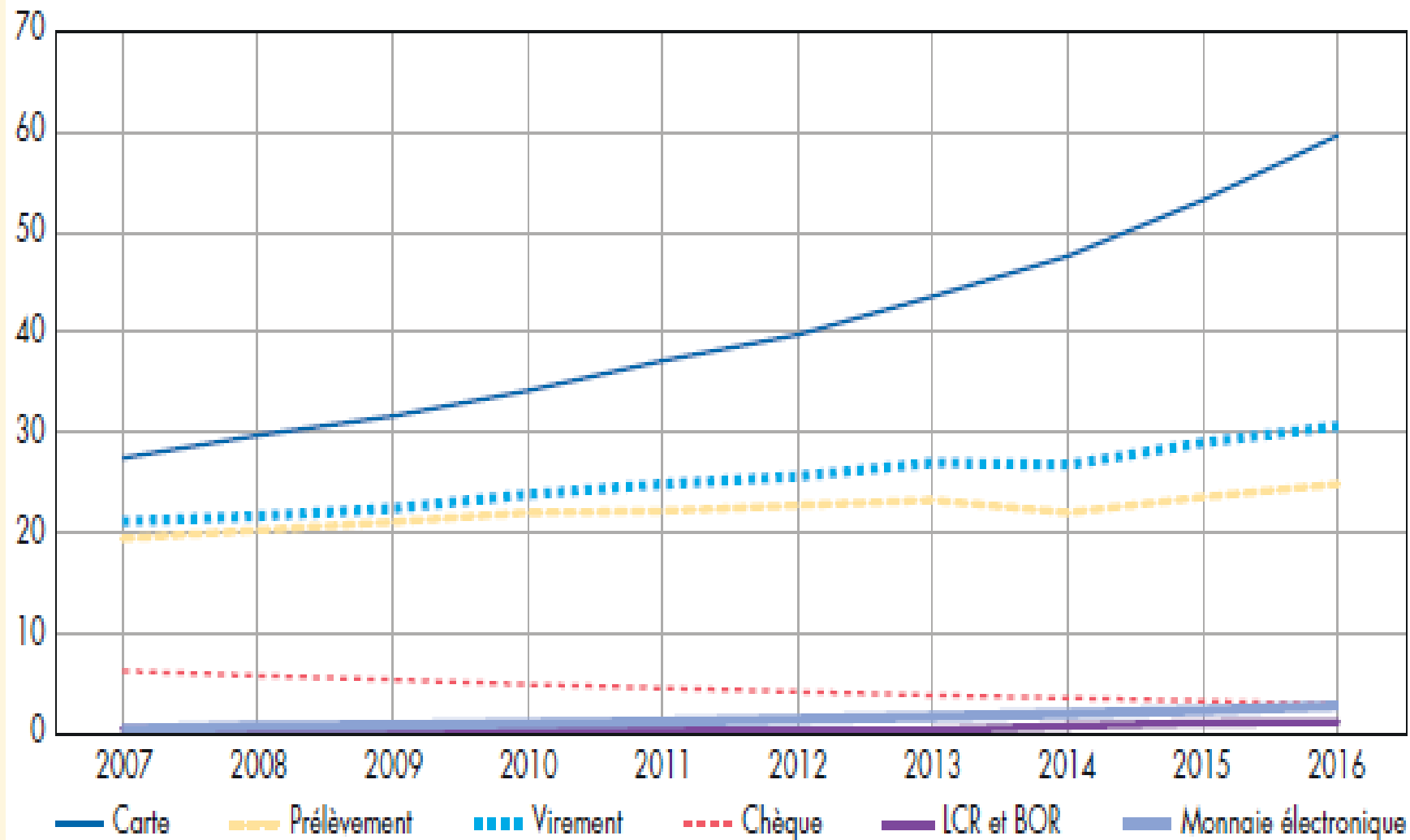
(en parts relatives)



**En moins de 10 ans, le volume des transactions par carte bancaire a plus que doublé dans l'Union européenne.**

## G4 : Évolution des moyens de paiement en volume dans l'UE

(en milliards de transactions)





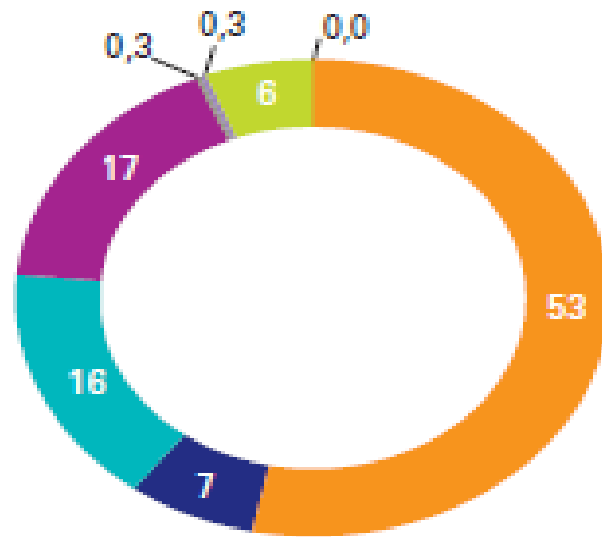
La France n'échappe pas à ce phénomène. Et ici comme dans l'Union européenne, on peut établir une différence entre nombre de transactions et valeur des transactions : les virements représentent 16% du nombre des transactions, mais 87% des montants.

C'est logique : le principal virement que nous recevons est notre salaire (ou retraite...)

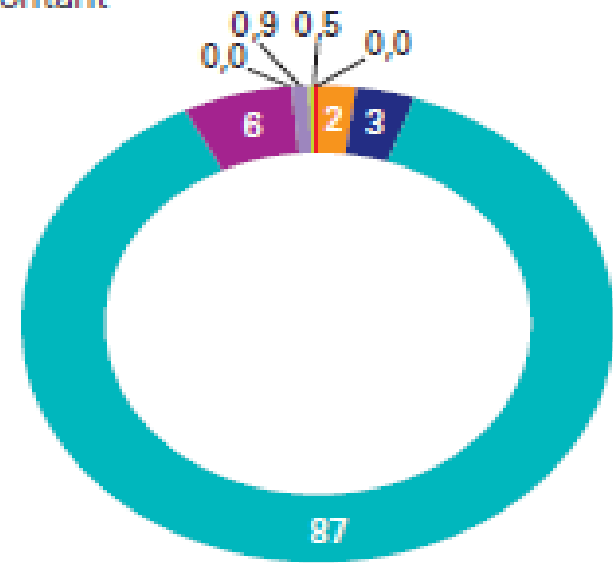
### G1 Usage des moyens de paiement scripturaux en France en 2018

(en %)

a) en volume



b) en montant



Paiement carte

Virement

Monnaie électronique

Retrait carte

Chèque

Prélèvement

Effet de commerce

SCT instantané <sup>a)</sup>

a) SCT instantané (SEPA instant credit transfer) : virement instantané.

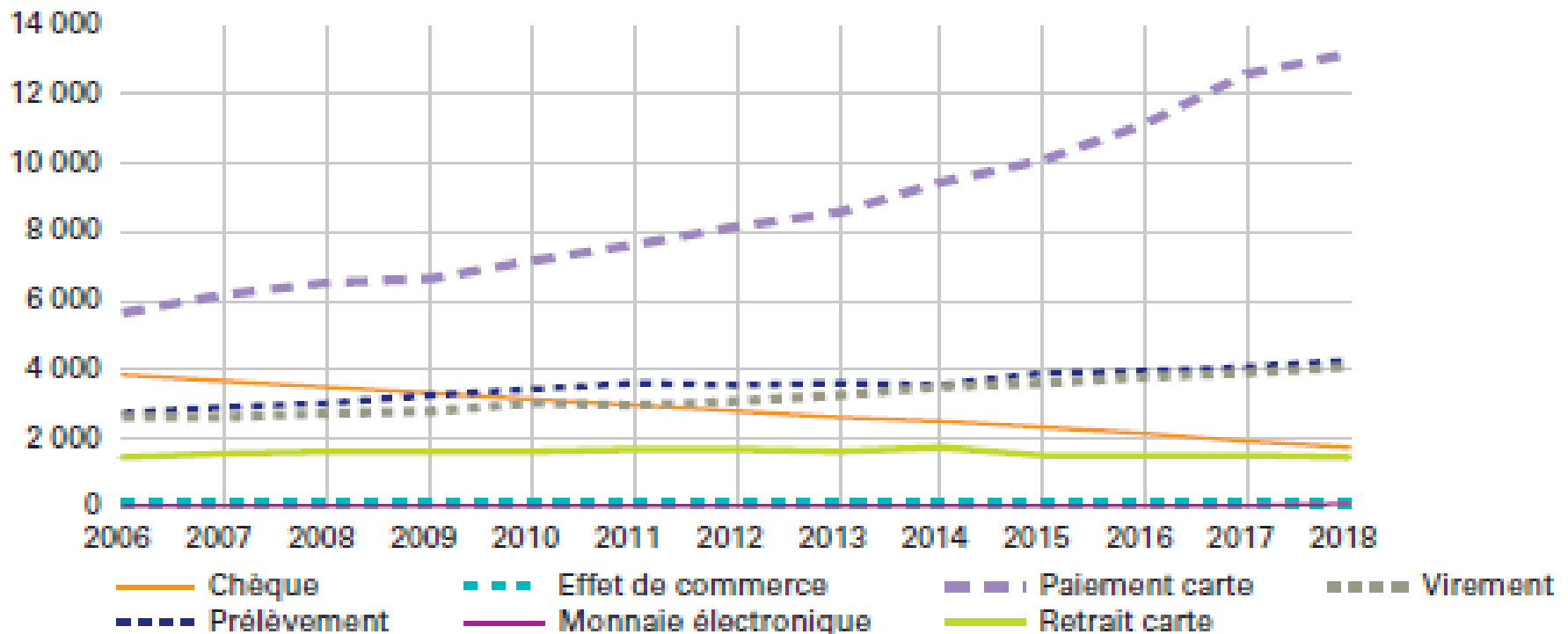
Source : Observatoire de la sécurité des moyens de paiement.

La progression du paiement par carte en France est un peu plus rapide que dans l'Union européenne et en 2018 13 milliards d'opérations de paiement ont été réalisées par carte.

Et on assiste au déclin rapide de tout ce qui peut nous rappeler la monnaie matérielle : les transactions par chèque ont diminué de moitié en 10 ans.

## G2 Usage des moyens de paiement en France depuis 2006

(en millions d'opérations)



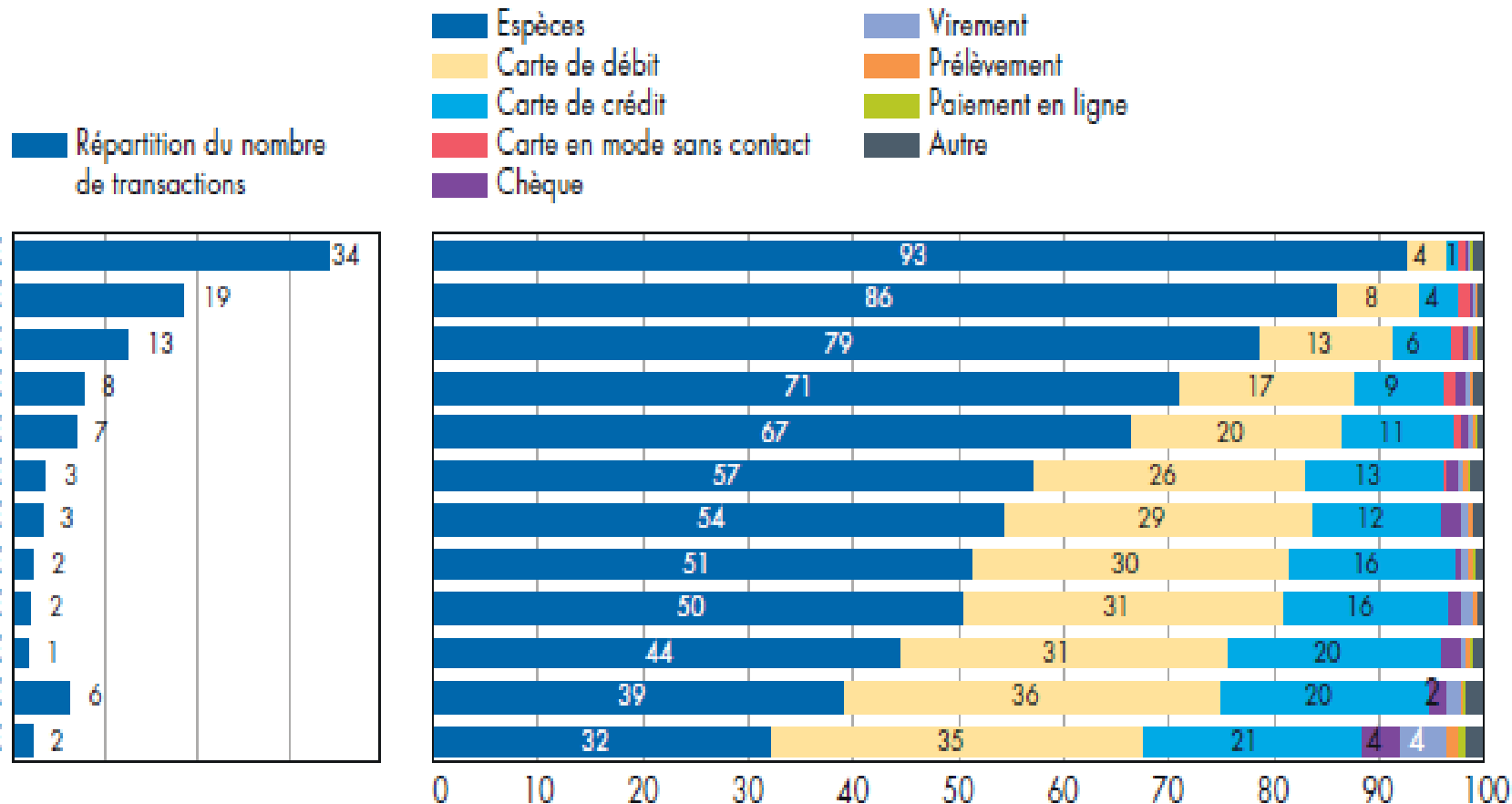
Source : Observatoire de la sécurité des moyens de paiement.

Bien entendu, les moyens de paiement restent très liés au montant à payer : pour les petites sommes, les espèces restent dominantes.

Mais le « sans contact » est en train de bouleverser cet élément.

### Encadré n° 2 : Utilisation des moyens de paiement au point de vente par tranche de montant en Europe

(en % du nombre de transactions)



**Tout ceci conduit à considérer que dans la masse monétaire totale de la zone euro, la monnaie « virtuelle » est ultra dominante.**

**La masse monétaire représente l'ensemble des moyens de paiement à un moment donné : on la classe de la plus liquide (la plus facile à utiliser) : M1, vers la moins liquide : M2 puis M3.**

**Les pièces et billets ne représentent plus que 14% de M1 et 9.4% de M3. Autant dire que la disparition de la monnaie matérielle ne représenterait pas un grand bouleversement de nos existences.**

**Cette disparition n'est pourtant pas totalement à l'ordre du jour : les gens ont encore un attachement un peu atavique à la monnaie réelle, surtout les personnes plus âgées qui se méfient des monnaies virtuelles.**

**Cela se remarque dans l'attachement des pays à conserver leurs réserves d'or : elles ne servent presque plus à rien, leur vente (surtout en ce moment) rapporterait beaucoup, mais aucun gouvernement ne semble vouloir renoncer à cette « ultime » protection.**

**M1 =**

Billets et pièces (Monnaie fiduciaire = 1 151,7 Mds €)  
+ Dépôts à vue sur des comptes courants  
(Monnaie scripturale<sup>1</sup> = 7 017,1 Mds €)  
**= 8 168,9 Mds €**

**M2 =**

M1 + Dépôts à terme et comptes sur livret d'une durée  
inférieure à 2 ans (3 408,2 Mds €)  
**= 11 577,1 Mds €**

**M3 (Masse monétaire) =**

M2 + Titres de créance (durée inférieure à 2 ans) = 621,1 Mds €  
**= 12 198,2 Mds €**

<sup>1</sup> Paiement par chèques, virements, paiements électroniques (carte bancaire, télépaiement).

**Nous pouvons visualiser la situation des moyens de paiement de la France en 2018, et constater que notre stock d'or représente à peu près 88 milliards d'euros, que nous pourrions injecter dans notre économie. Mais, bien entendu, on ne le fera pas : ce n'est pas de l'économie, c'est de la psychologie.**



## Chiffres clés en 2018



66

millions de transactions quotidiennes en moyens de paiement scripturaux



75,5

milliards d'euros échangés quotidiennement via les moyens de paiements scripturaux



58%

la part des cartes dans le nombre de transactions scripturales, contre 33% pour les moyens de paiement SEPA et 8% pour le chèque



140,0

milliards d'euros, les avoirs en or et en devises nets des passifs en devises, DTS compris (vs 133 milliards en 2017)



52,2

milliards d'euros, le montant des réserves en devises (actifs nets des passifs en devises, DTS compris)



87,8

milliards d'euros, l'évaluation des réserves en or de la France (2436 tonnes d'or)

Malgré ces quelques résistances de la monnaie matérielle, la dématérialisation de celle-ci va continuer, et la révolution numérique va grandement accélérer ce phénomène.

La carte bleue est elle aussi promise à voir son rôle diminuer petit à petit : elle sera remplacée dans un premier temps par le téléphone portable et les applications qu'il contiendra (on les appelle les « token ») et qui permettront de payer, y compris à distance, par avance...

On pourra également payer « à l'œil » (sans vouloir faire de jeux de mots) : c'est notre iris qui permettra de valider des transactions monétaires.

La reconnaissance faciale jouera également : il suffira par exemple de passer par un sas qui nous reconnaîtra pour que nos paiements soient immédiatement enregistrés (au niveau des autoroutes par exemple).

Bref, le numérique sera partout dans nos moyens de paiement. Mais la sécurité de ces transactions va devenir un enjeu essentiel.

## 2 Numérique, monnaie et sécurité.

Bien entendu, les voleurs et les fraudeurs ne sont pas apparus avec les moyens de paiement numérique. Mais ceux-ci vont leur offrir de nouvelles opportunités :

- les cartes bancaires peuvent être dérobées, mais surtout piratées à distance ou tout simplement par des yeux indiscrets (ou des téléphones portables qui les prennent en photos).

- sur internet, les fraudes et arnaques peuvent se multiplier. Le plus inquiétant est le piratage direct des données bancaires sur son ordinateur à l'aide des fameux cookies.

- les moyens de paiement par téléphones peuvent être interceptés par d'autres téléphones.

Les voleurs d'aujourd'hui sont souvent moins violents que ceux d'autrefois, mais ils sont aussi beaucoup plus malins. Et la généralisation des achats sur internet va considérablement accélérer le processus de risque de fraude : les achats sont anonymes.



## E-COMMERCE EN EUROPE

# 547

milliards d'€ en 2018

1 346 € par acheteur en 2018

source : Ecommerce Foundation.

+ 11.9%  
par rapport  
à 2017

## E-COMMERCE DANS LE MONDE

# 2 131

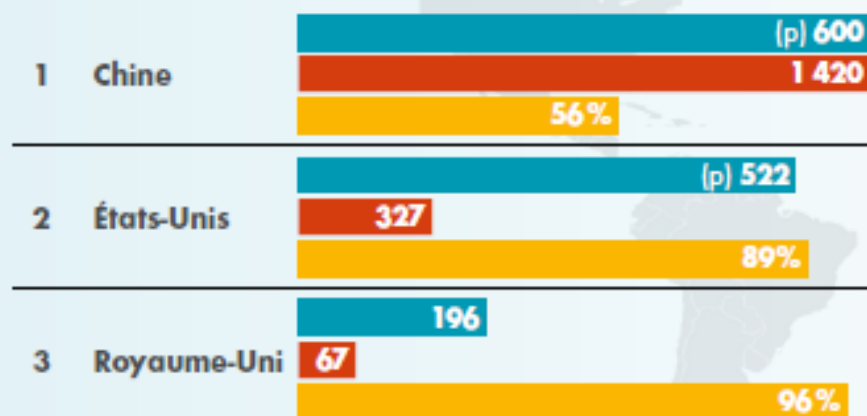
milliards d' \$ en 2018 (p)

(p) : prévisions

source : Ecommerce Foundation.

+ 14.3%  
par rapport  
à 2017

### Top 3 des pays dans le monde

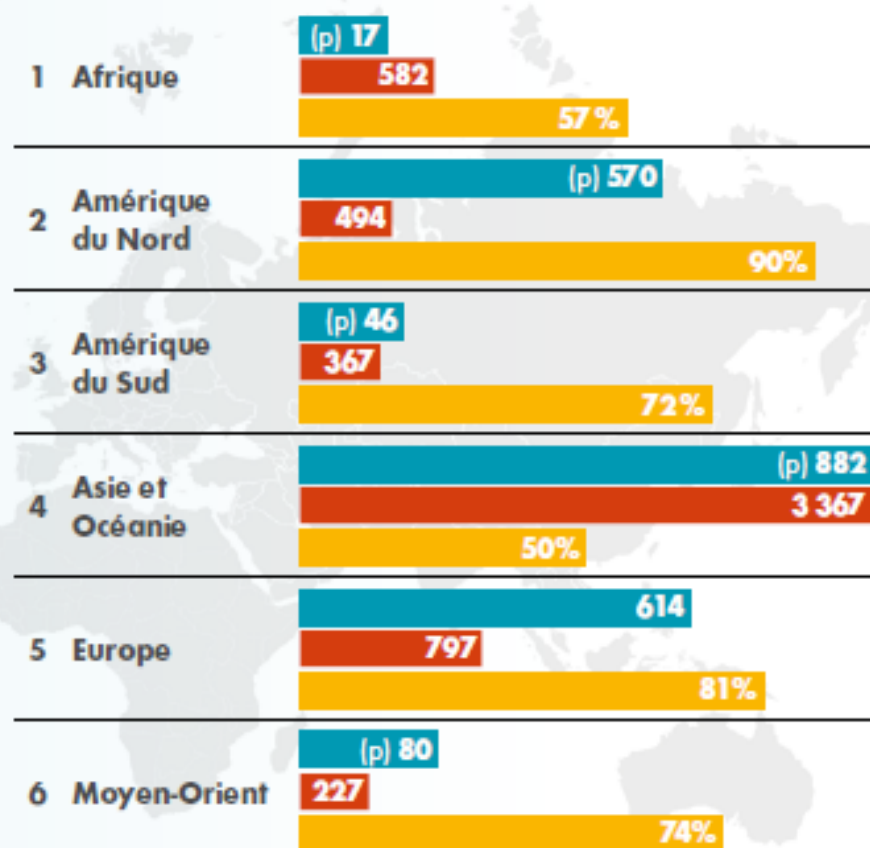


### Top 4 des pays

1	Royaume-Uni	174.9
2	France	92.6
3	Espagne	28
4	Italie	27.4

Allemagne : ND. Chiffre d'affaires e-commerce BtoC 2018 en milliards d'€.

source : Ecommerce Foundation.



Chiffre d'affaires e-commerce BtoC 2018 en milliards de \$- (p) Prévisions. Population en millions d'habitants Pénétration d'internet

source : Ecommerce Foundation.

## T1 : Les quatre grandes typologies de fraude aux différents instruments de paiement

Typologie de fraude	Carte de paiement	Chèque	Virement	Prélèvement
<b>Faux</b>	<ul style="list-style-type: none"> <li>Utilisation par le fraudeur d'une carte perdue ou volée à son titulaire légitime ou d'un numéro de carte usurpé (vente à distance)</li> <li>Fausse carte créée par un fraudeur à partir de données qu'il a recueillies</li> </ul>	<ul style="list-style-type: none"> <li>Utilisation par le fraudeur d'un chèque perdu ou volé à son titulaire légitime</li> <li>Faux chèque, créé de toutes pièces par un fraudeur, émis sur une banque existante ou une fausse banque</li> </ul>	<ul style="list-style-type: none"> <li>Transmission par le fraudeur d'un faux ordre de virement</li> <li>Usurpation des informations de connexion à un espace bancaire en ligne pour initier des virements frauduleux</li> </ul>	<ul style="list-style-type: none"> <li>Émission par le fraudeur d'un ordre de prélèvement sans mandat ou à partir d'un faux mandat</li> </ul>
<b>Falsification</b>	<ul style="list-style-type: none"> <li>Carte authentique dont les données magnétiques, d'embossage <sup>a)</sup> ou de programmation ont été modifiées par le fraudeur</li> </ul>	<ul style="list-style-type: none"> <li>Chèque régulier intercepté par le fraudeur qui l'altère par grattage, gommage ou effacement</li> </ul>	<ul style="list-style-type: none"> <li>Virement régulier intercepté et modifié par le fraudeur</li> </ul>	<ul style="list-style-type: none"> <li>Remplacement des références du compte du créancier légitime par celles du compte du fraudeur sur un ordre ou fichier de prélèvement</li> </ul>
<b>Détournement</b>	<ul style="list-style-type: none"> <li>Paiement ou retrait sous la contrainte</li> </ul>	<ul style="list-style-type: none"> <li>Chèque régulier signé par le titulaire légitime sous la contrainte ou la manipulation</li> </ul>	<ul style="list-style-type: none"> <li>Virement initié, par le titulaire légitime du compte, sous la contrainte ou par la tromperie vers un compte qui n'est pas celui du bénéficiaire légitime ou qui ne correspond à aucune réalité économique</li> </ul>	<ul style="list-style-type: none"> <li>Usurpation par le fraudeur de l'identité et l'IBAN d'un tiers pour la signature d'un mandat de prélèvement sur un compte qui n'est pas le sien</li> </ul>
<b>Utilisation/ contestations abusive</b>	<ul style="list-style-type: none"> <li>Contestation abusive par le porteur d'une transaction de paiement par carte valide qu'il a initiée</li> </ul>	<ul style="list-style-type: none"> <li>Chèque émis par le titulaire légitime, de manière abusive, à partir d'une formule authentique qu'il a préalablement déclarée perdue ou volée</li> </ul>	<ul style="list-style-type: none"> <li>Contestation abusive par le titulaire du compte d'un ordre de virement valide qu'il a initié</li> </ul>	<ul style="list-style-type: none"> <li>Contestation abusive par le débiteur d'un ordre de prélèvement émis légitimement par le créancier (litige commercial)</li> </ul>

a) Modification de l'impression en relief du numéro de carte.

**La fraude aux moyens de paiement reste encore marginale quand on la rapporte à l'ensemble des transactions effectuées : elle ne représente « que » 0.062% des transactions par carte bancaire, et 0.0004% des virements bancaires.**

**Si la fraude la plus courante se fait par carte bancaire (90% des cas de fraude), en montant c'est le chèque qui reste le plus impacté (43% du montant des fraudes, le chèque sans provision n'étant pas considéré comme une fraude).**

**Mais les sommes en jeu deviennent importantes et pénalisent à la fois les clients, les banques, les commerçants et l'ensemble de la sphère productive.**

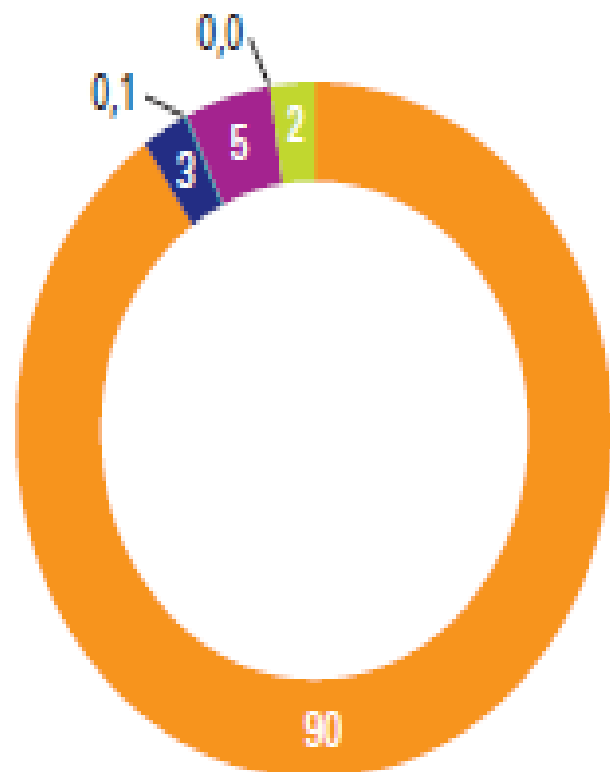
**Les transactions par carte bancaire représentent 704 milliards € en France en 2018 (+ 55% depuis 2009), et le montant des fraudes par cartes 439 millions € (+ 65%).**

**La fraude progresse donc plus vite que les transactions et les sommes sont loin d'être négligeables.**

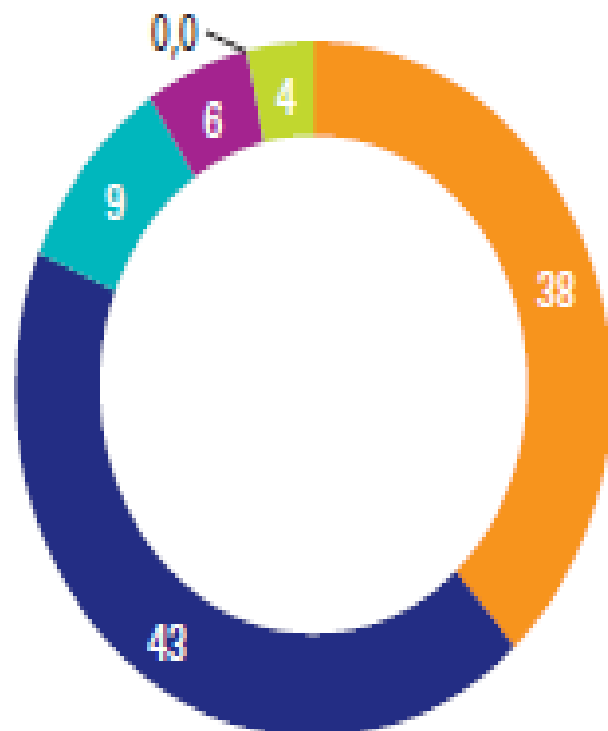
## G5 Répartition de la fraude sur les moyens de paiement scripturaux en 2018

(en %)

a) en volume



b) en montant



Paiement carte

Chèque

Virement

Prélèvement

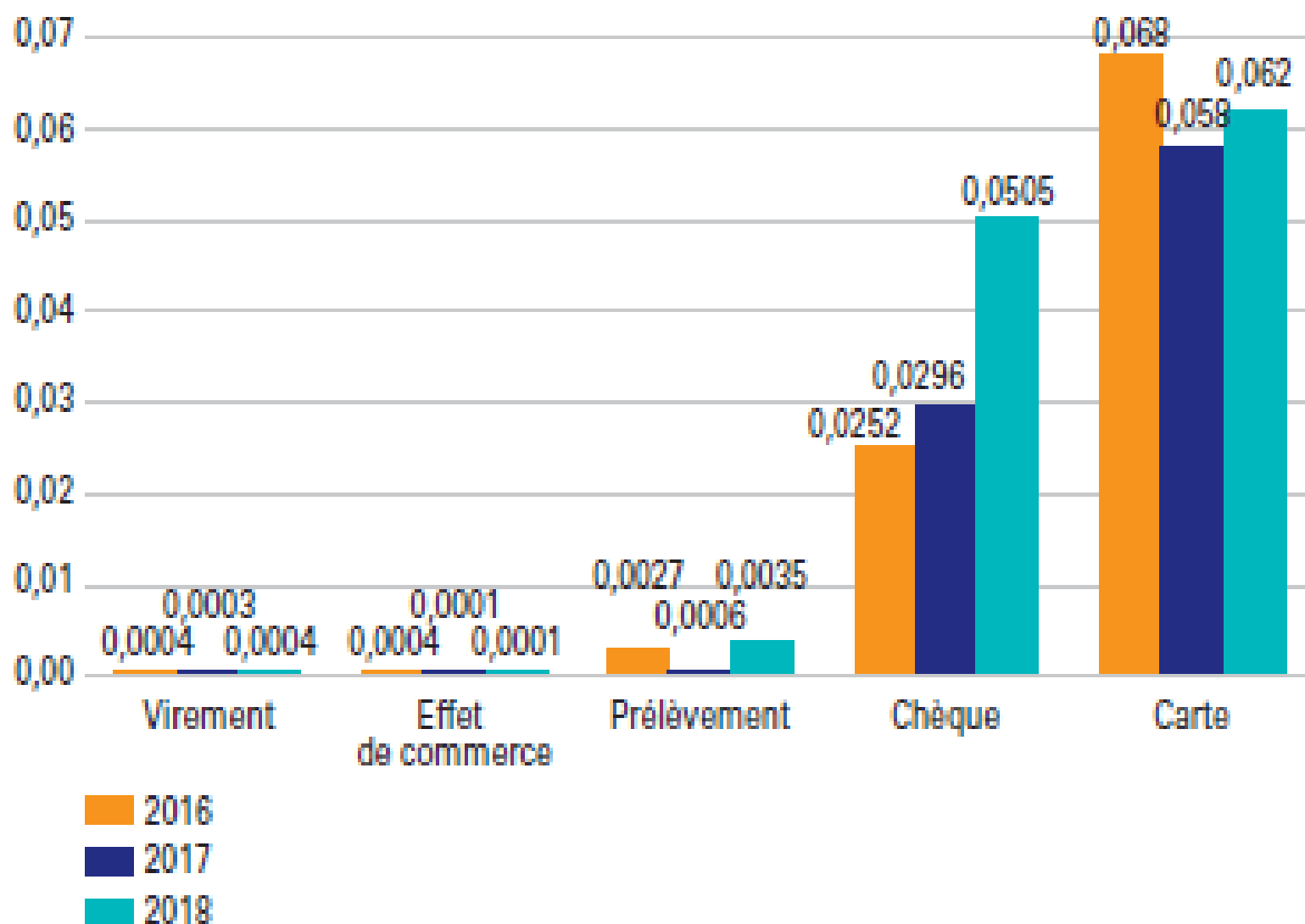
Effet de commerce

Retrait carte

Source : Observatoire de la sécurité des moyens de paiement.

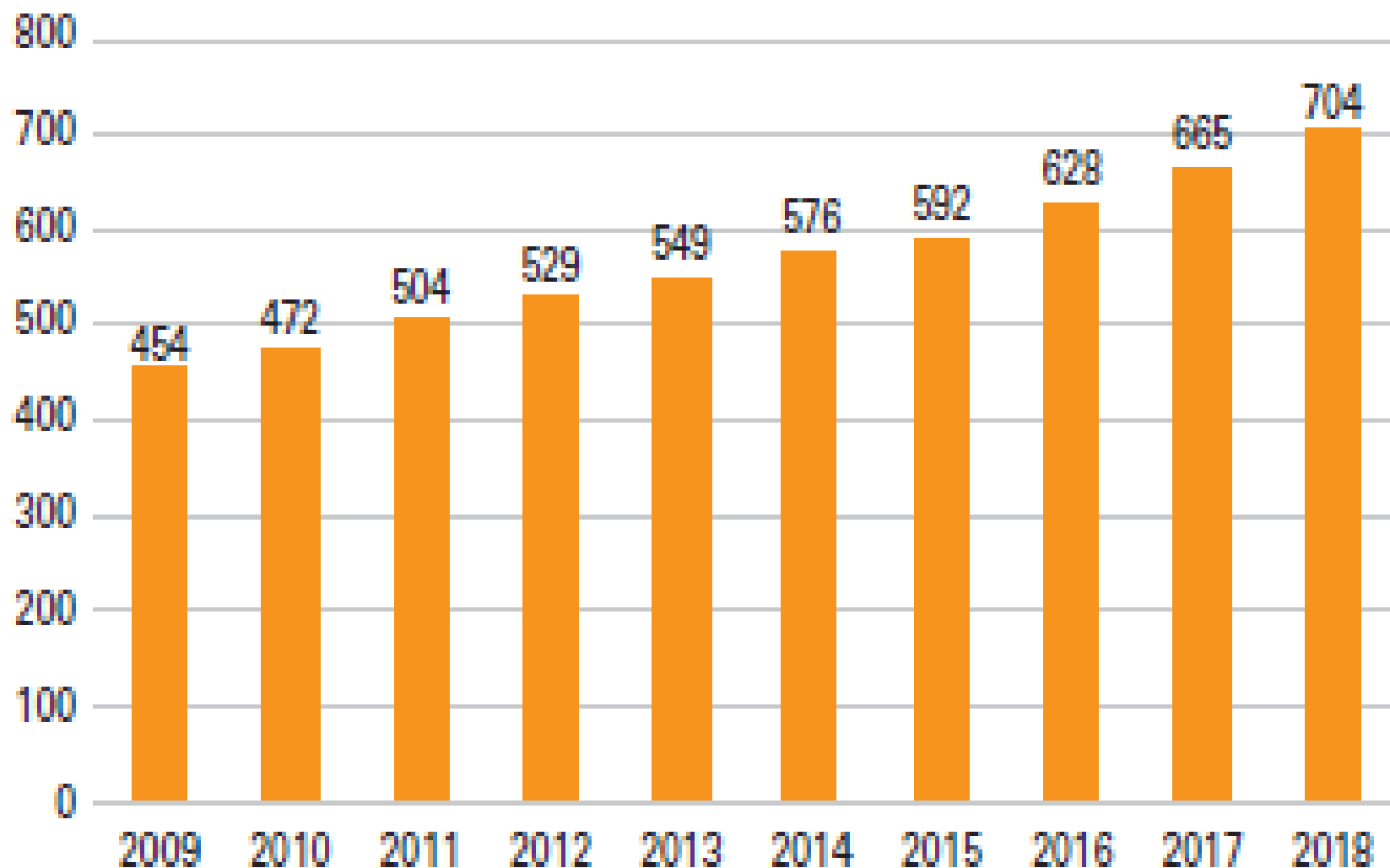
## G6 Évolution du taux de fraude par moyen de paiement, de 2016 à 2018

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

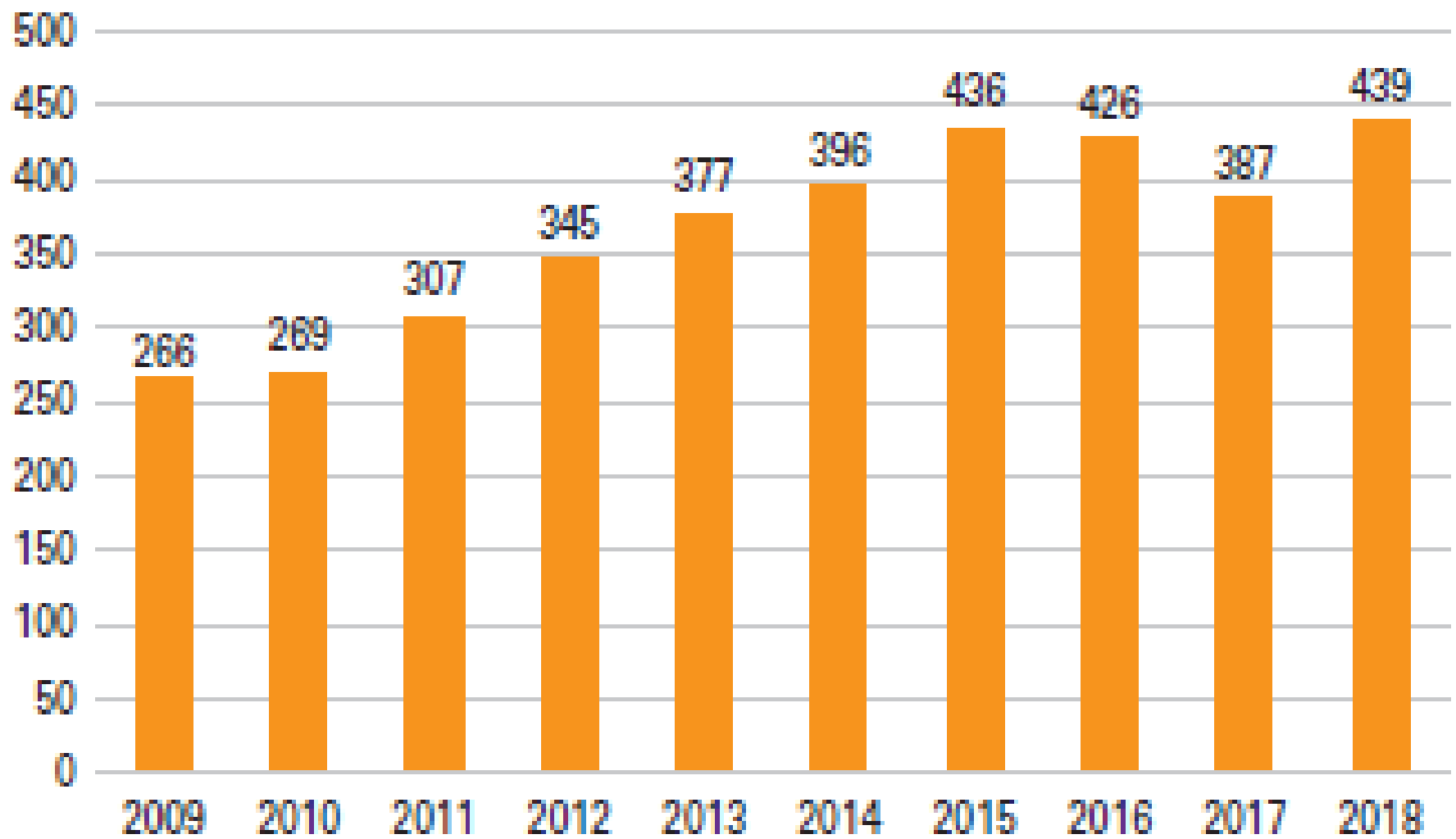
## G7 Montant total des transactions des cartes françaises (en milliards d'euros)



Source : Observatoire de la sécurité des moyens de paiement.

# G8 Montant total de la fraude des cartes françaises

(en millions d'euros)

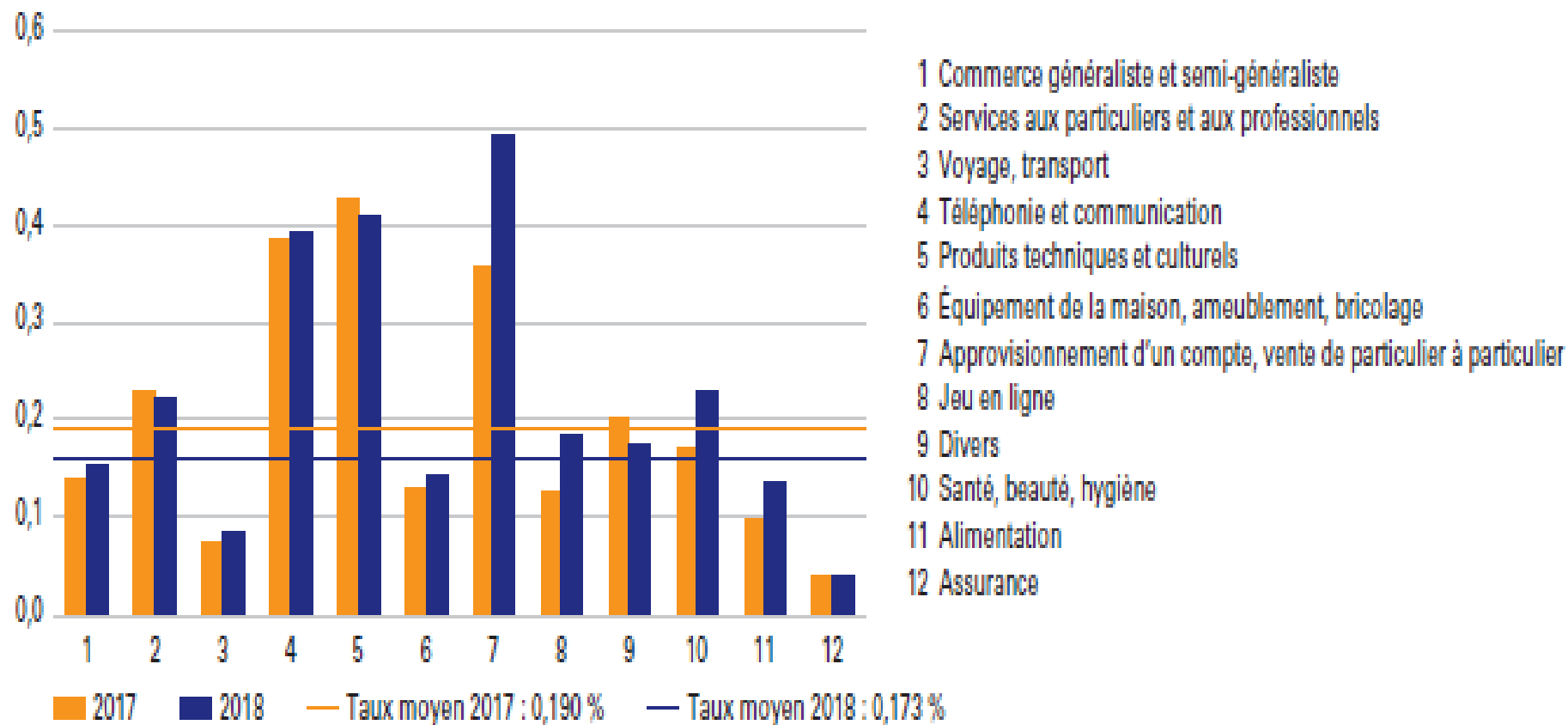


Source : Observatoire de la sécurité des moyens de paiement.

En matière de vente à distance (par internet le plus souvent), les cas de fraude les plus fréquents concernent la téléphonie et les communications, l'achat de produits culturels, la vente entre particuliers et les ordres de virement à un compte.

### Taux de fraude en vente à distance par secteur d'activité, transactions nationales

(en %)



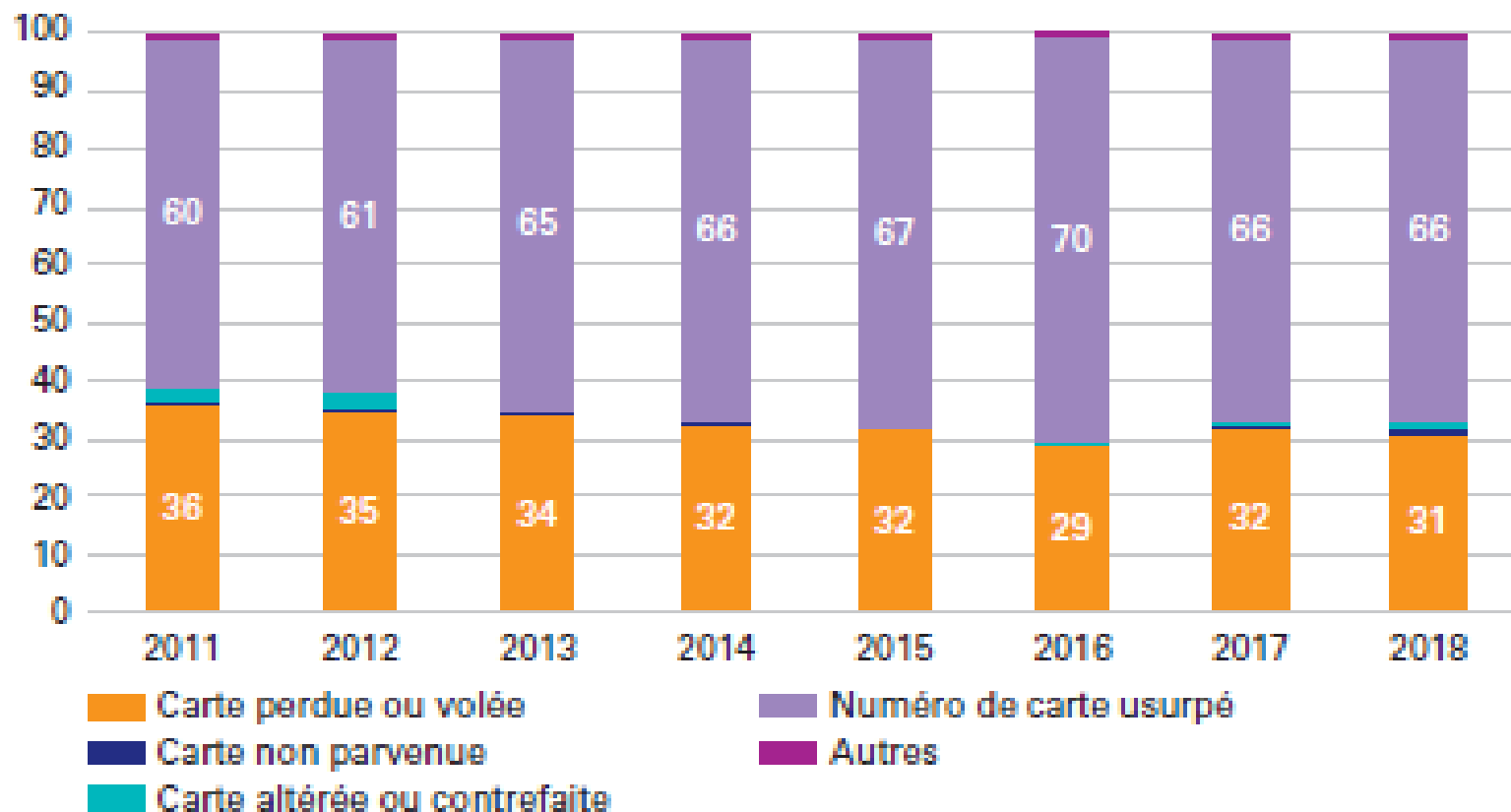
Source : Observatoire de la sécurité des moyens de paiement.



La carte est l'instrument de paiement le plus souvent fraudé. Il s'agit en particulier de l'usurpation du numéro de carte (de plus en plus souvent sur internet) ou de la perte ou vol de la carte elle-même.

## G17 Répartition de la fraude aux paiements par carte selon la typologie de fraude

(en %)



Note : Transactions nationales hors retraits, en valeur.

Source : Observatoire de la sécurité des moyens de paiement.

Face au développement de ces nouveaux moyens de paiement, et face aux nouveaux voleurs et fraudeurs, le système bancaire, appuyé par les banques centrales, a donc du réagir.

En matière de vente à distance, le moyen désormais le plus utilisé est le « 3D-Secure » rendu obligatoire par une directive européenne du 1<sup>o</sup> novembre 2009 (DSP1).

La banque de l'acheteur doit faire identifier l'ordre d'achat par son client avant de valider la transaction en question.

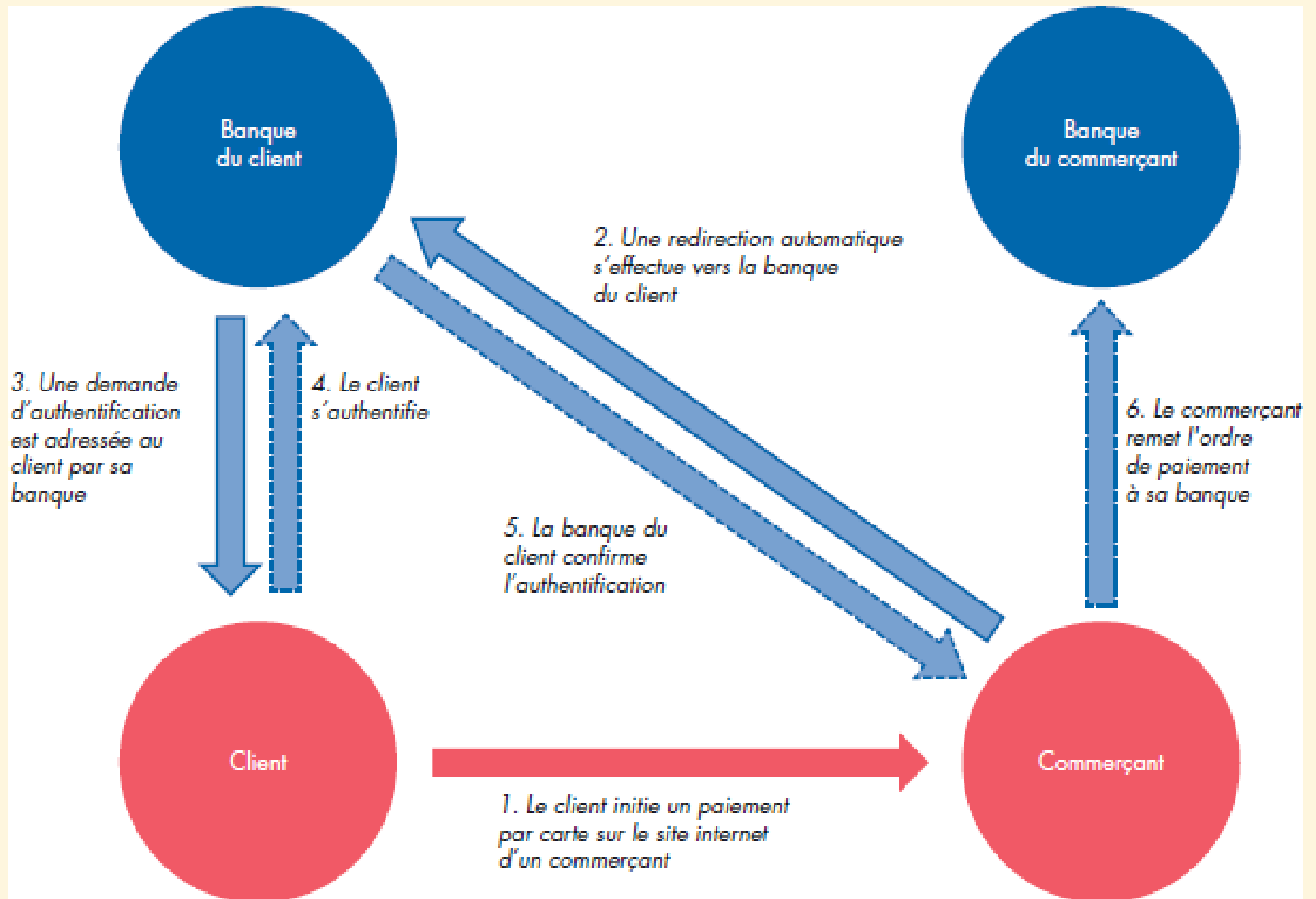
La plupart du temps, cela se fait par réception d'un code de validation qu'il faut ensuite recopier pour valider la transaction.

Mais d'ores et déjà, cela ne semble plus suffire pour au moins trois raisons :

- c'est inopérant en cas de vol de carte quand le voleur dispose également du téléphone de la victime

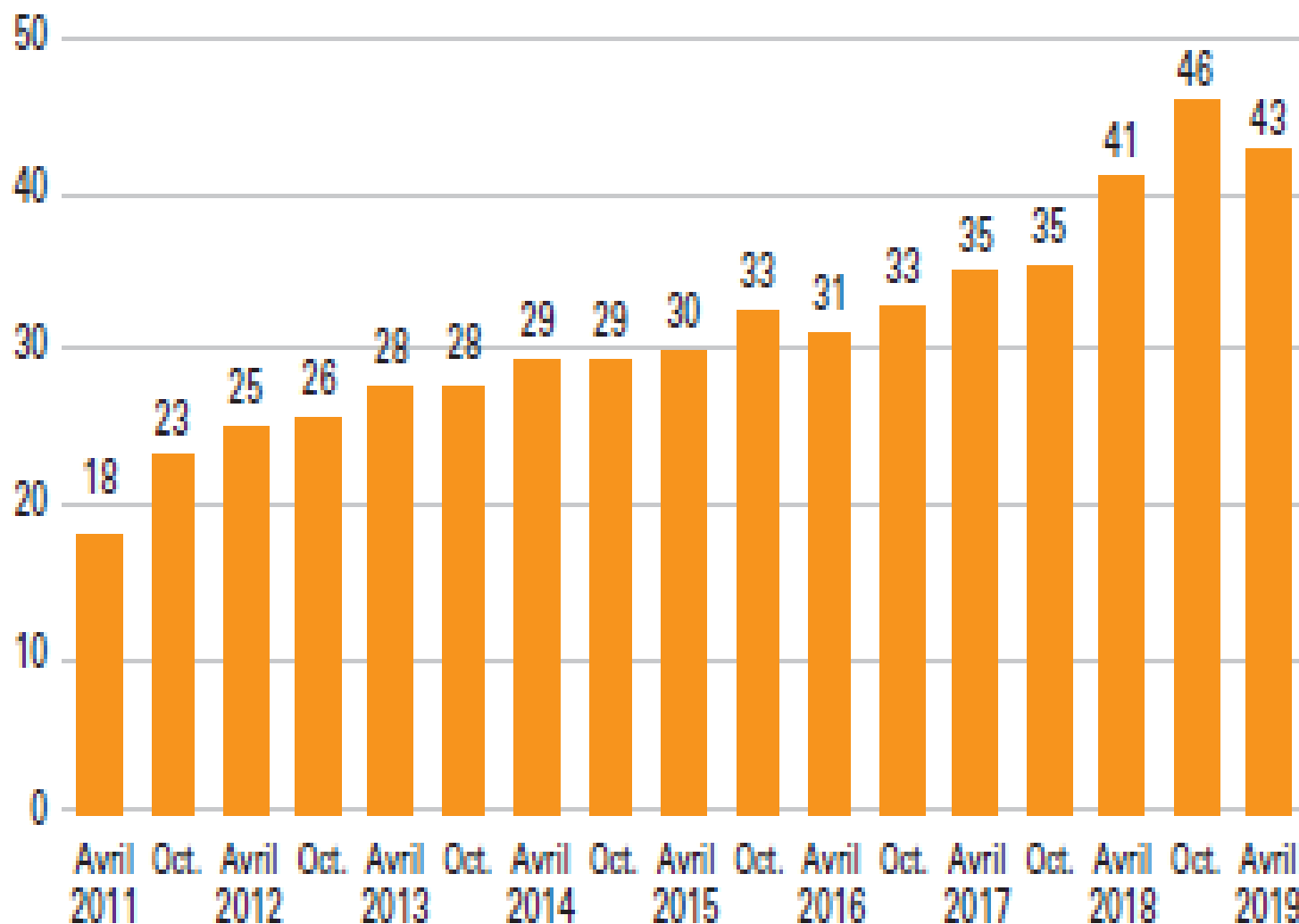
- 43% seulement des paiements en ligne sont protégés par 3D-Secure

## Fonctionnement du protocole « 3D-Secure »



## G21 Part du montant total des paiements en ligne authentifiés par 3D-Secure

(en %)



Source : Observatoire de la sécurité des moyens de paiement.

- et puis surtout, rien ne permet d'indiquer que la personne qui reçoit le code et qui valide la transaction soit la « bonne » personne : là également les moyens d'interception électronique se multiplient.

Face à cela, deux réactions :

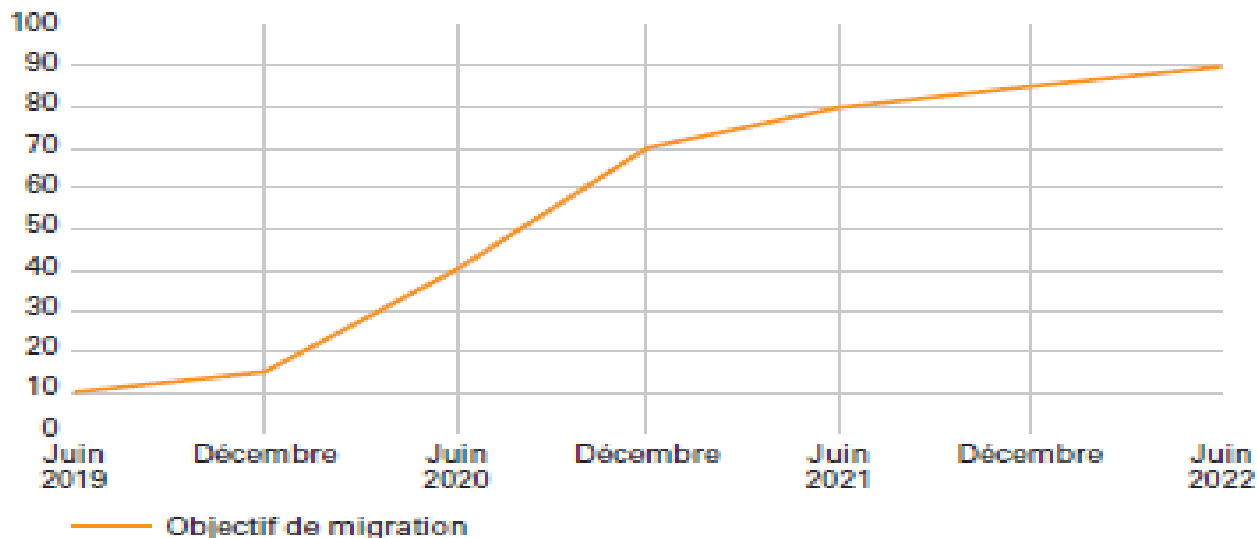
- une directive européenne exige depuis le 13 janvier 2018 la migration des moyens de paiement vers une authentification plus forte : l'objectif est de parvenir à 100% en 2022 (DSP2).

Votre banque va donc vous demander (elle l'a peut-être déjà fait) de lui fournir une identification forte qu'elle pourra redemander au moment des transactions, et qui sera beaucoup plus difficilement « piratable » (une reconnaissance faciale par exemple).

- les banques utilisent de plus en plus le « big data » : elles archivent vos paiements et vos habitudes, pour essayer de détecter par des algorithmes des opérations suspectes (réalisées à l'étranger, à des heures inhabituelles, sur des achats non habituels...).

## G1 Enrôlement des clients

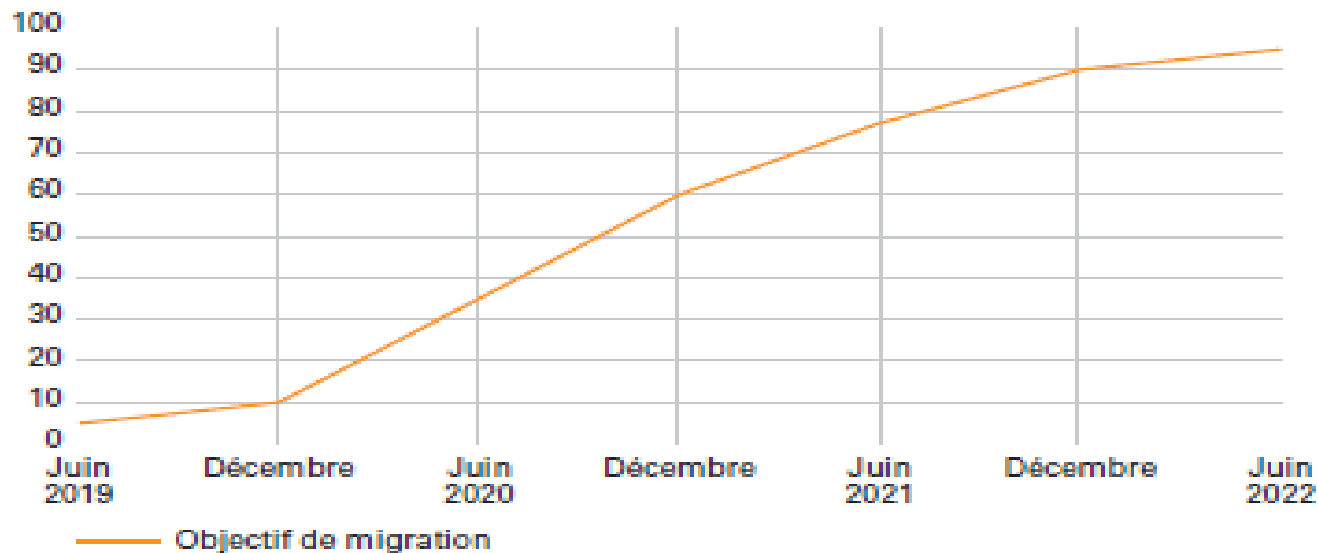
(en %)



Source : Observatoire de la sécurité des moyens de paiement.

## G2 Authentification des paiements requérant une SCA

(en %)



Note : SCA (*strong customer authentication*) : authentification forte du client.

Source : Observatoire de la sécurité des moyens de paiement.

Reste le problème principal : celui du paiement à partir du téléphone portable, qui va se généraliser.

Or ce téléphone est très sensible aux vols, et surtout au piratage et à l'interception des données.

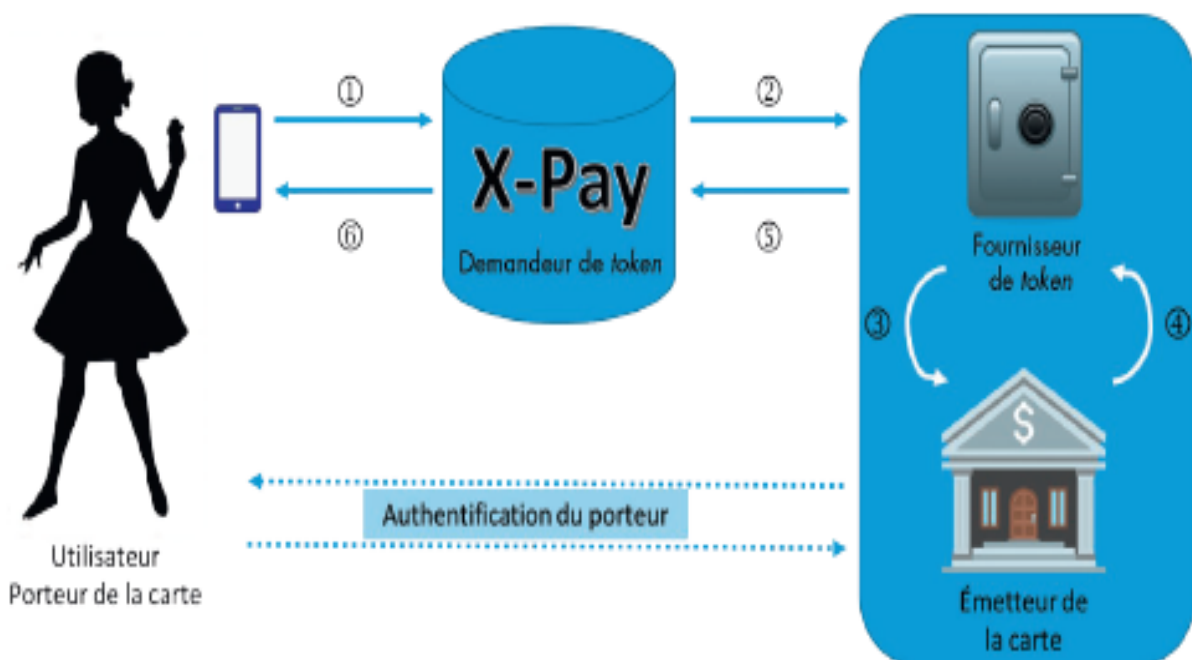
Pour sécuriser ce mode de paiement, la technologie va s'appuyer sur la même technologie que celle des crypto-monnaies : la blockchain.

Pour payer, le téléphone devra émettre une demande de « token », c'est-à-dire une autorisation de sa banque via un fournisseur. Ce token sera généré par une série de vérification mathématiques instantanées qui rendent le piratage beaucoup plus difficile.

En gros, à chaque étape de la blockchain, il est posé une question mathématique complexe que seule l'application du téléphone est censée résoudre, sur la base d'une clé initiale.

Quand le token sera accepté, la transaction par téléphone pourra se faire. Le tout se passe, bien entendu, en l'espace de moins d'une seconde.

## Tokenisation d'une carte



1. Pour enrôler une nouvelle carte, l'application mobile émet une demande de *token* contenant les données d'identification de la carte, à savoir son numéro, sa date d'expiration et son cryptogramme visuel.
2. Le TR (*token requestor*, demandeur de *token*) demande la génération d'un *token* au TSP (*token service provider*, fournisseur de *token*) de la banque émettrice de la carte.
3. Le TSP demande à l'émetteur de valider la demande, notamment en vérifiant les données de la carte et si celle-ci n'est pas en opposition.
4. L'émetteur valide la demande de *token*.

5. Après avoir généré un nouveau *token*, le TSP transmet celui-ci au TR.

6. Le TR transmet le *token* à l'application mobile pour qu'elle puisse l'utiliser en lieu et place du numéro de la carte enrôlée.

Lors de cette opération, l'émetteur demande généralement à son porteur de s'authentifier en confirmant qu'il est bien à l'origine de la demande de *token*. Cette phase peut être mise en place de différentes manières, suivant le portefeuille électronique.



### 3 Vers une guerre des crypto-monnaies ?

Une crypto-monnaie n'est pas une véritable monnaie : elle n'est pas émise (et donc garantie) par une banque centrale et elle peut parfaitement être refusée comme moyen de paiement.

Néanmoins, elles se développent (2 238 crypto-monnaies dans le monde actuellement) car elles présentent trois avantages :

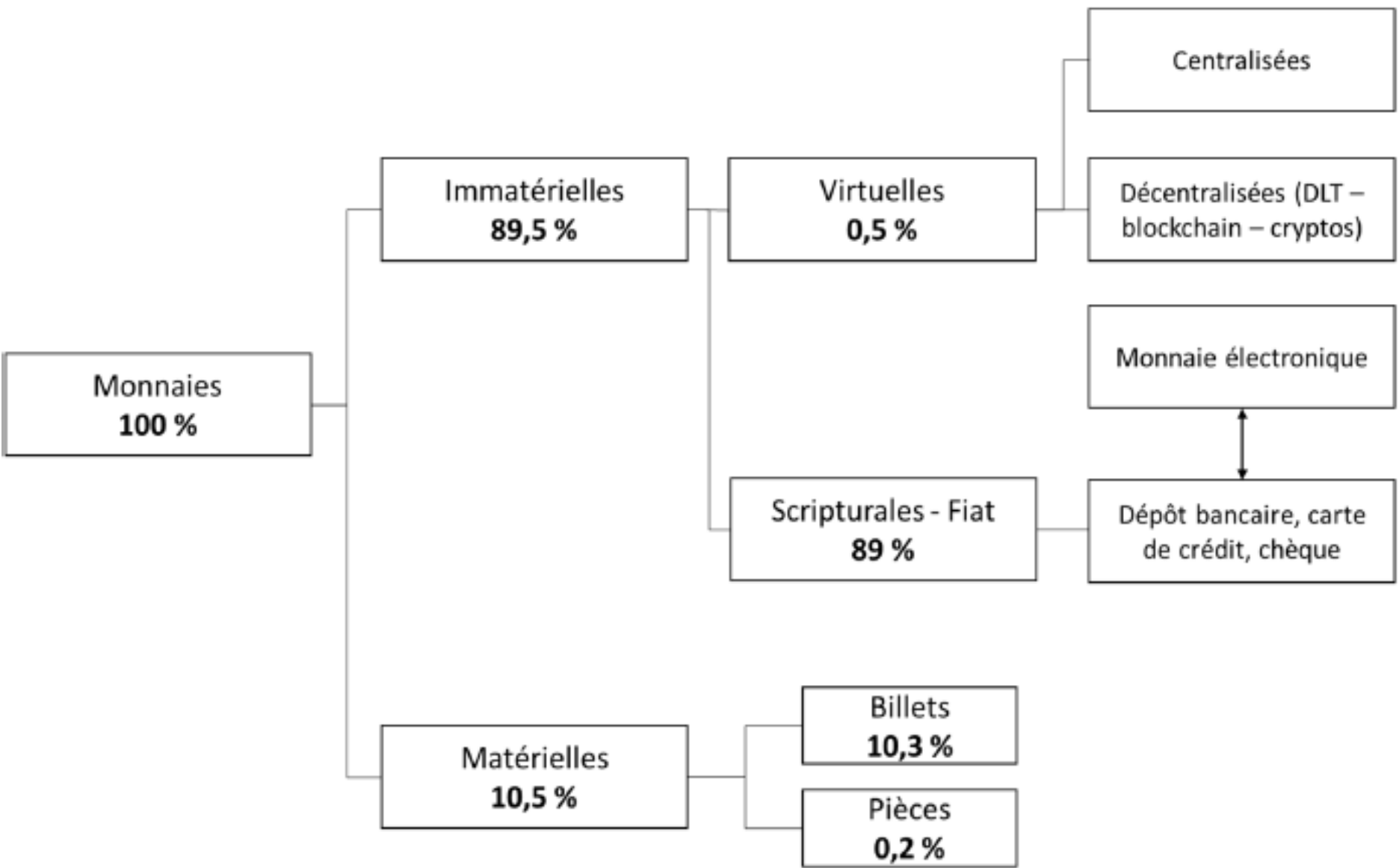
- au niveau des transactions d'un montant élevé, elles sont beaucoup plus sécurisées que les transactions classiques, du fait des vérifications en série provoquées par la blockchain.

- elles sont beaucoup plus rapides dans leur transmission que les ordres de virement classiques, puisqu'elles ne passent pas par le système bancaire, mais par des paiement « pair à pair ».

- elles sont beaucoup plus discrètes, à l'abri du regard des banques, des banques centrales et des gouvernements.

Pour le moment, elles ne représentent qu'une part infime des transactions monétaires.

Elles ne représentent que 0.5% des moyens de paiement, mais surtout elles vont être concurrencées par une nouvelle forme de crypto-monnaie : celle contrôlée par les banques centrales.





**1.** Alix soumet la transaction, cryptée avec sa clé privée, au réseau pair-à-pair.



**2.** Les mineurs authentifient la transaction : ils vérifient que la clé privée correspond à l'adresse d'Alix, qu'Alix possède bien

les 5 Bitcoins et qu'elle n'en a pas consacré certains à une autre transaction.



**3.** La transaction est regroupée avec d'autres transactions chronologiquement dans un bloc.



**4.** Les mineurs sont en concurrence pour valider le bloc en résolvant un problème mathématique (\* preuve de travail \*).



**1 Bis.**  
Elle envoie sa clé publique à Bernard.

## ALIX VEUT ENVOYER 5 BITCOINS À BERNARD



**8.** La transaction est validée et Bernard reçoit les Bitcoins.



**7.** L'enregistrement génère de nouveaux Bitcoins, versés au mineur qui a trouvé la solution.



**6.** Une fois approuvé, le bloc est horodaté et certifié par une empreinte numérique (« hash »), puis ajouté à la chaîne de blocs existante.

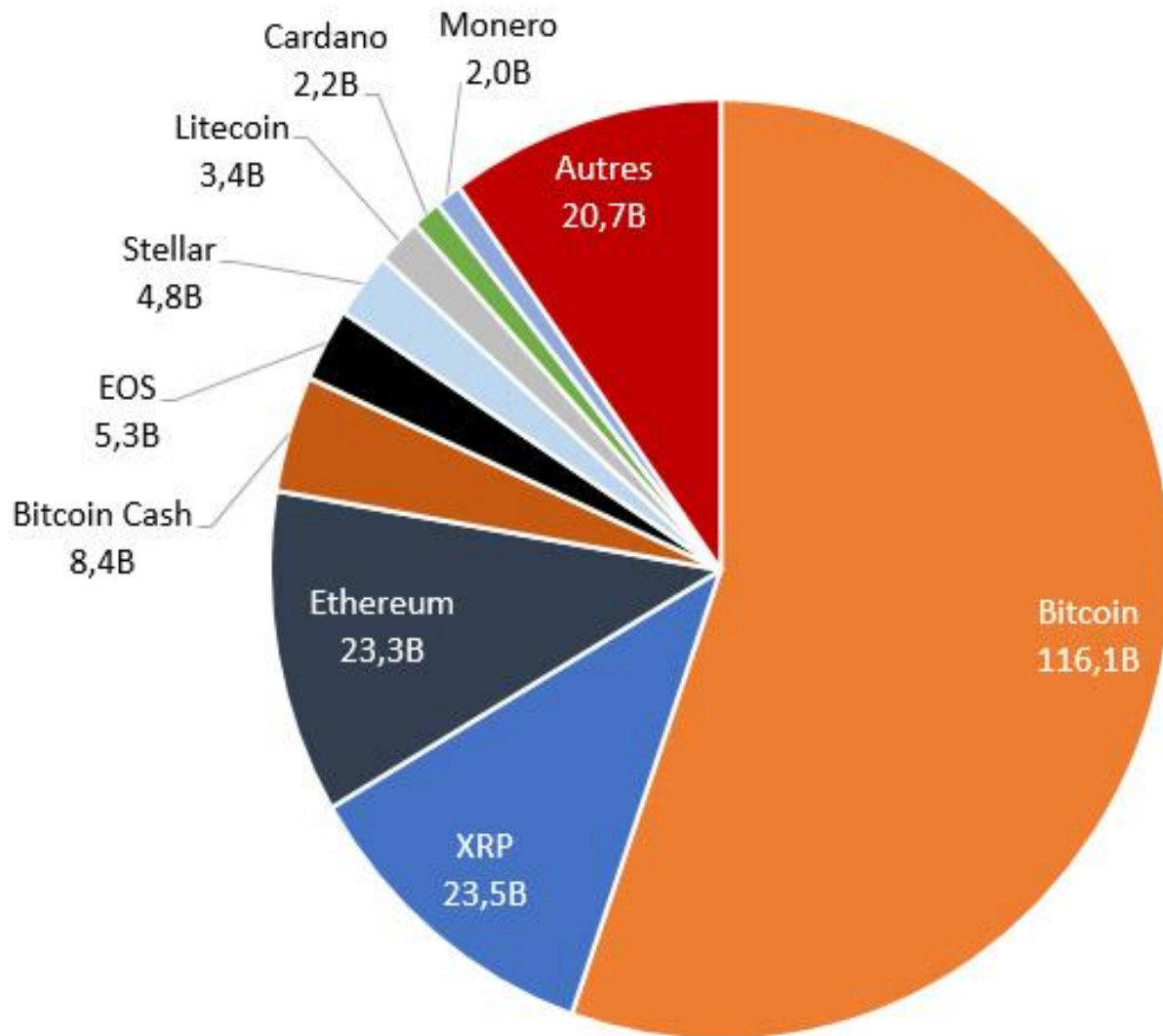


**5.** Quand un mineur a trouvé la solution, il la soumet aux autres mineurs, qui pourront la vérifier facilement.

# Le Bitcoin, ancêtre des crypto-monnaies, représente à lui seul 55.2% du total des cryptomonnaies

Principales crypto-monnaies par capitalisation de marché.

Source: Coin Market Cap, 2018.



# Nouvel emballement en vue pour les cryptomonnaies ?

■ Nombre de cryptomonnaies différentes ● Capitalisation boursière en Mds \$



**Mercredi 4 décembre 2019, François Villeroy de Galhau, le gouverneur de la Banque de France, a annoncé l'expérimentation, dès 2020, d'une Monnaie Digitale de Banque Centrale (MDBC).**

**Beaucoup d'autres banques centrales devraient suivre ou précéder : la Chine s'apprête elle aussi à lancer sa monnaie digitale : l'e-couronne.**

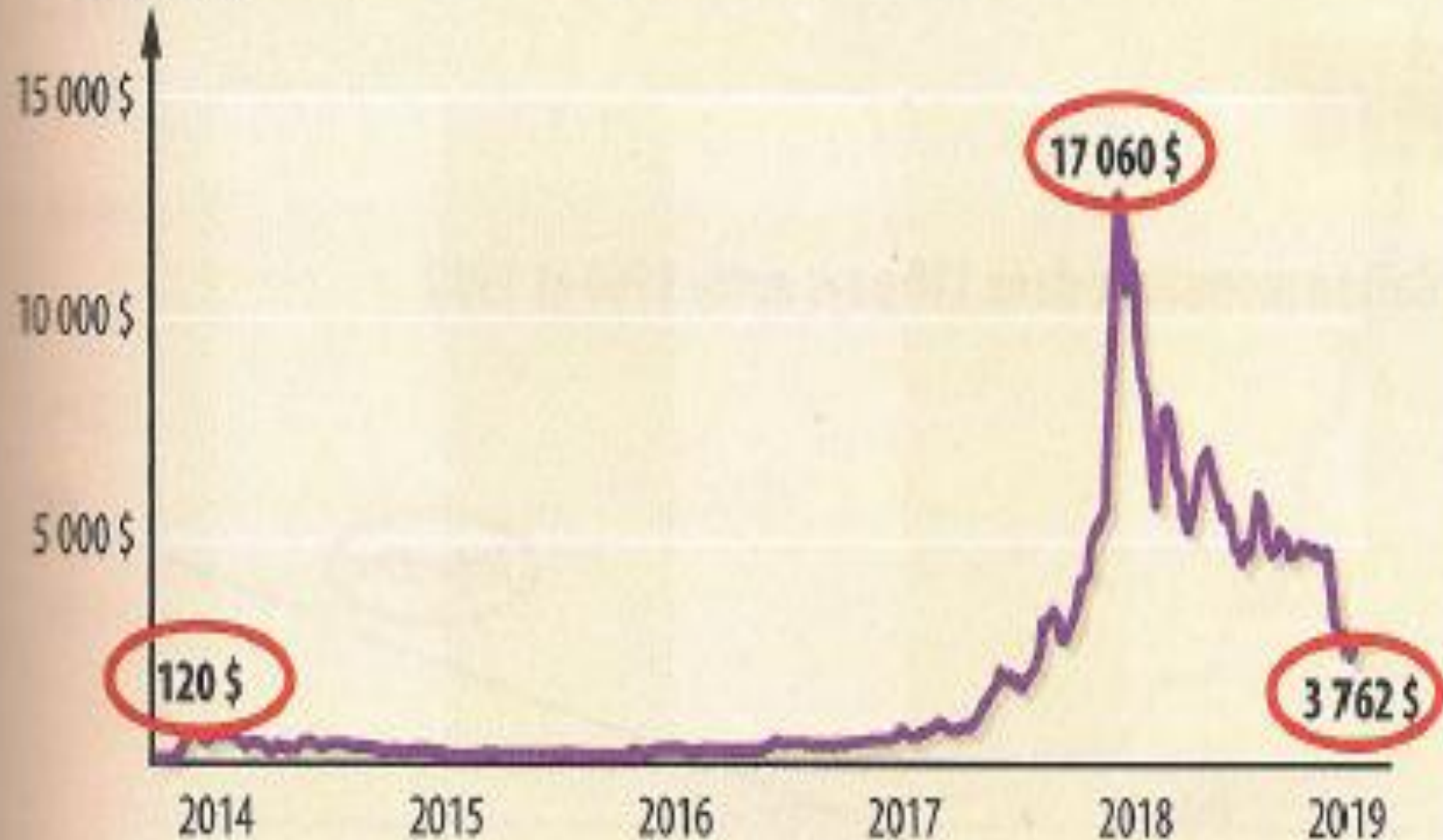
**Plusieurs éléments poussent les banques centrales à agir :**

- sur le plan conjoncturel, c'est l'annonce faite par Facebook de lancer sa monnaie digitale (le Libra) qui a convaincu les banques centrales du caractère probablement irréversible de ce mouvement : difficile de rester à l'écart (même si le Libra a du mal à se concrétiser).**

- les crypto-monnaies sont très volatiles et sensibles à la spéculation, à l'image du Bitcoin : les banques centrale voudraient donc essayer d'en adopter le principe, tout en contrôlant toutefois les spéculations les plus visibles.**

## Évolution du cours du bitcoin

En dollars



Source : [www.coindesk.com](http://www.coindesk.com).

- les banques centrales constatent également que les échanges de crypto-monnaies se concentrent dans quelques pays seulement, dont certains sont assez peu coopératifs en matière de renseignements financiers.

C'est donc une double perte pour les pays plus « classiques » : perte financière et pertes fiscales.

Tableau 2 : Classement des cinq principaux pays en fonction des volumes d'échanges journaliers sur les plateformes de crypto-monnaies

Mars 2018	Juin 2018
1. Hong Kong (31 %)	1. Hong Kong (30 %)
2. États-Unis (29 %)	2. Malte (26 %)
3. Corée du Sud (15 %)	3. États-Unis (11 %)
4. Royaume-Uni (14 %)	4. Royaume-Uni (11 %)
5. Japon (5 %)	5. Singapour (10 %)

Source : Mission, d'après JP Morgan, mai 2018, et cryptocoincharts, juin 2018.



- et puis, quoique plus sécurisées que les transactions « classiques », les crypto-monnaies ne sont pas à l'abri de cyber-attaques qui peuvent faire perdre des centaines de millions.

L'idée des banques centrales est donc d'essayer de participer à ce marché, pour le rendre encore plus inviolable qu'actuellement.

Bien entendu, les crypto-monnaies « privées » ne sont pas d'accord.

#### Encadré 4 : Historique des principales cyber-attaques et sur le marché des crypto-monnaies depuis 2014

- Titanium : 21 millions de dollars (avril 2018) ;
- LoppX : 4,5 millions de dollars (février 2018) ;
- Coincheck : 530 millions de dollars (janvier 2018) ;
- PlexCoin : 15 millions de dollars (décembre 2017) ;
- Bitfinex : 72 millions de dollars (août 2016) ;
- Bitstamp : 5,2 millions de dollars (janvier 2015) ;
- Mt. Gox : 487 millions de dollars (février 2014).

Source : Morgan Stanley.

Entre les crypto-monnaies, il va donc y avoir un double combat :

- entre les crypto-monnaies privées entre elles pour conserver (Bitcoin) ou acquérir (Libra ?) une supériorité d'utilisation.
- entre les crypto-monnaies privées et celles bientôt générées par les banques centrales pour dominer le marché et surtout imposer des standards de fonctionnement.

Pour le grand public, pour le moment, tout ceci nous concerne d'assez loin. Mais on ne peut pas exclure l'hypothèse d'un développement important de ce type de « monnaies libres » comme moyen classique de paiement.

Ces crypto-monnaies seront surtout un complément aux monnaies classiques, en cas d'échanges monétaires importants via internet.

Et elles risquent de jouer un rôle décisif au niveau des moyens de paiement sans contact, en particulier au travers de la téléphonie mobile. La dématérialisation de la monnaie n'est donc sans doute pas achevée.