PAIEMENTS 2030

Comment paierons-nous en France dans la prochaine décennie ?

pa eu
the payments association

THIBAULT DE BARSY, VICE-CHAIRMAN & GENERAL MANAGER
THE PAYMENTS ASSOCIATION EU

Mot d'introduction

Le paiement est le système sanguin de notre économie. Les Français aspirent à ce qu'on simplifie leur vie et leurs transactions monétaires. Qu'il s'agisse d'un contrat d'exportation ou d'un café au comptoir, chacun doit pouvoir disposer de la meilleure technologie disponible, aujourd'hui et demain.

Pour anticiper la France des paiements en 2030, nous voulions confronter le mieux-disant technologique de tous les acteurs actifs en Europe. Mastercard nous a permis d'accéder à ses meilleures ressources pour regrouper la grande famille des paiements autour de quatre tables rondes sur des technologies d'avenir ayant servi de base à nos travaux :

- Blockchain – Vers une économie du token ? *(12 septembre 2023)*
- Biométrie – Le corps humain, dernière frontière des paiements ? *(10 octobre 2023)*
- IoT – Vers des paiements autonomes ? *(16 novembre 2023)*
- Quantique – Sécuriser les paiements à l'ère du quantique *(7 décembre 2023)*

Ces réflexions ont par la suite été complétées par des contributions des membres de la Payments Association EU pour aboutir à un large panorama du futur de notre industrie.

Bien entendu, ce document n'a pas vocation à être exhaustif et aurait pu couvrir de multiples autres technologies, mais il offre une première vision de ce que pourrait être le futur des paiements.

Ce livre blanc présente une vision de certains des défis et opportunités technologiques que rencontrera l'industrie des paiements, en ce compris les autorités réglementaires et le secteur public. Bien entendu, ce document n'a pas vocation à être exhaustif et aurait pu couvrir de multiples autres technologies, mais il offre une première vision de ce que pourrait être le futur des paiements.

Nous espérons avant tout qu'il sera utile, en tant que source d'information mais aussi d'outil de planification stratégique.

NIMA SEPASY, SENIOR VICE PRESIDENT INNOVATION, INSIGHTS & ENGAGEMENT, MASTERCARD

Interview

1. Comment envisagez-vous l'avenir des paiements ?

Notre façon de payer deviendra plus intuitive, interactive, immersive, et intégrée à notre vie quotidienne, et notre définition de la monnaie aura vocation à s'élargir pour inclure des actifs non traditionnels. On constate aujourd'hui que les technologies de réseau s'améliorent déjà au niveau de l'architecture, des normes et des transmissions de données afin d'apporter des expériences plus intelligentes dans les magasins, les bureaux et les environnements industriels.

L'utilité des données s'accroît encore davantage pour créer de nouvelles formes de valeur. Nous nous éloignons de l'échange de l'argent classique pour inclure de nouveaux actifs tels que les points de fidélité, les données, les biens numériques, les droits et les nouvelles monnaies. La tokenisation des actifs permet d'accéder à cet éventail plus large d'actifs tout en favorisant la confiance et la sécurité dans l'échange. À mesure que nous évoluerons vers un monde tokenisé, les consommateurs et les entreprises pourront utiliser, combiner et échanger de nouvelles formes de valeur, libérant ainsi des richesses inexploitées et créant de nouveaux modèles d'entreprise.

Alors que ces tendances se développent, elles continueront de stimuler la croissance et la transformation dans l'ère numérique. Le défi pour les industries sera de naviguer stratégiquement dans ces évolutions et de garantir que l'intégration de ces technologies serve des objectifs commerciaux plus larges.

2. Comment Mastercard s'adapte à ces changements ?

Mastercard ne s'adapte pas à ces changements, nous les menons. Nous travaillons déjà avec des technologies émergentes et les employons pour protéger plus de 143 milliards de transactions chaque année. Nos équipes, s'engagent à développer des solutions pratiques qui intègrent la confidentialité et l'éthique dès la conception et adhèrent aux normes les plus élevées en matière de sécurité. À travers nos capacités, nous nous assurons que la confiance est au premier plan et que la technologie est utilisée de manière responsable et éthique. En embrassant le changement technologique tout en relevant ses défis, nous pouvons entrer dans l'avenir du commerce et veiller à ce que la technologie influence positivement le monde.

Notre programme d'innovation nous permet d'être bien positionnés pour soutenir nos clients et nos partenaires lorsque des tendances et des technologies émergentes apparaissent. Nous menons en permanence des recherches, testons de nouvelles technologies, incubons de nouvelles solutions, concevons l'interface utilisateur et réduisons les risques de mise en œuvre. Nous nous concentrons sur la construction de prototypes pour acquérir une compréhension approfondie des technologies émergentes telles que l'IA et l'IA générative, mais aussi la quantique, l'AR/VR, les PET (preuves d'exécution de la transaction) et plus encore.

3. Selon vous, quelle est la technologie qui apportera les changements les plus importants ?

L'IA a le potentiel d'être un puissant catalyseur pour le commerce en améliorant l'analyse des données pour des perspectives inégalées, en personnalisant et en rationalisant chaque expérience, et en protégeant l'économie mondiale avec une sécurité sans pareille. Nous continuons de percevoir des opportunités dans les manières dont l'IA permet aux expériences numériques d'être encore plus intelligentes, plus sûres et plus personnalisées.

L'intérêt public pour l'IA générative est resté fort depuis son émergence explosive il y a plusieurs années. Les entreprises expérimentent rapidement avec les outils d'IA générative pour améliorer la productivité, la créativité et les expériences client. Mais nous n'avons qu'effleuré la surface de ce que l'IA générative est capable d'accomplir, notamment dans l'industrie des paiements.

Une journée en 2030

Nous sommes en 2030. Marie est une jeune employée vivant et travaillant en France.

07:00

Après s'être levée, Marie consulte son réfrigérateur intelligent. Celui-ci a **automatiquement passé commande pour les produits manquants grâce à des contrats intelligents, le paiement ayant été validé par reconnaissance biométrique** et sécurisée.

07:30

Pour se rendre à son bureau, Marie utilise sa voiture autonome connectée qui intègre un système de paiement embarqué. Sur le trajet, **les frais de transport sont calculés en temps réel, les péages et les parkings sont automatiquement débités de son portefeuille numérique crypto** à la fin du trajet.

08:00

Juste avant d'aller récupérer son café, Marie passe une commande activée par la voix depuis sa voiture. **Son paiement est automatiquement effectué lorsque la commande est prête.** Dès qu'elle arrive, son café l'attend à la table qu'elle a réservée.

12:00

Pour le repas, Marie et ses collègues se rendent dans un restaurant où les paiements intégrés sont omniprésents. Elle commande via une tablette présente à sa table, fixe la caméra et **le paiement est sécurisé automatiquement grâce à un scan rétinien.** A la fin du repas, Marie effectue un paiement de compte à compte pour payer sa partie.

18:00

En rentrant de son travail, Marie s'arrête à un magasin qui utilise la blockchain pour la gestion de la chaîne d'approvisionnement. Elle prend un **panier intelligent qui détecte automatiquement les articles ajoutés et les paiements sont traités instantanément.** Elle sort sans avoir à attendre à la caisse ou même déballer ses produits.

19:00

Rentrée chez elle, il est l'heure de se détendre. En effectuant des achats en ligne, à l'aide de son portefeuille numérique, elle utilise des dispositifs IoT sécurisés et ses choix sont guidés par un assistant digital de calculateur d'empreinte carbone. **Les informations de paiement sont directement intégrées dans les dispositifs,** facilitant des transactions rapides et sécurisées.

23:00

Avant de se coucher, Marie consulte son portefeuille numérique et envoie un paiement transfrontalier immédiat à ses parents qui sont en vacances en Espagne. Elle **valide l'accès à ses comptes financiers par reconnaissance faciale.** Les données sont cryptées et protégées par des technologies de sécurité post-quantique, et les transactions sont enregistrées de manière transparente sur une blockchain. Marie utilise également des **applications de finance décentralisée (DeFi) pour gérer ses investissements et ses épargnes.**

Paiements 3.0 - Perspectives pour la décennie à venir

Infrastructures – Des rails interopérables pour répondre à tous les usages

Le paiement, outil fondamental pour révolutionner le commerce

L'industrie des paiements, et le commerce en général, a connu ces dernières décennies des transformations majeures et rapides, marquées par des innovations de rupture. Ces évolutions peuvent en grande partie être attribuées à l'essor d'internet qui a facilité le partage immédiat d'informations et aboli les limites du monde physique.

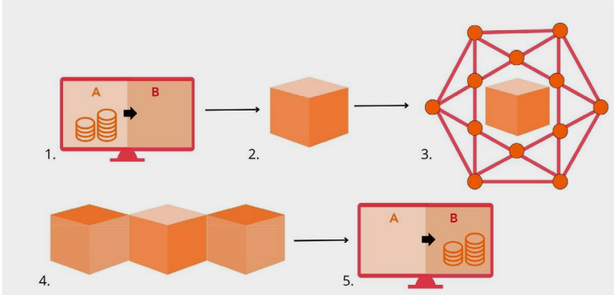
Le paiement, et notamment les cartes bancaires, ont été un outil incontournable dans cette révolution, permettant des échanges rapides, simples et sécurisés entre les commerçants et les consommateurs. Une grande partie des sites e-commerce et des applications mobiles reposent ainsi sur une infrastructure de carte bancaire permettant de finaliser la transaction. Selon Statista, la carte est d'ailleurs le moyen de paiement le plus utilisé sur internet. En effet, 84 % des e-acheteurs ont utilisé la carte bancaire au cours des 12 derniers mois de l'année 2023[1].

Le secteur des paiements continue d'évoluer en permanence pour s'adapter aux attentes des utilisateurs. Malgré cela, il existe toujours certains défis, en particulier au niveau international, pour atteindre l'immédiateté souhaitée des transactions, ce qui conduit à des initiatives visant à améliorer l'infrastructure des paiements.

Blockchain et tokenisation, nouvelle étape dans la numérisation des paiements ?

Face à ces défis liés aux paiements internationaux, la blockchain est souvent présentée comme une infrastructure alternative qui pourrait permettre de réduire les délais de règlement tout en limitant le nombre d'intermédiaires.

Conceptualisée en 2008 dans le cadre de la création du Bitcoin, la blockchain est une technologie de stockage et de transmission d'informations dont la promesse est d'être transparente, hautement sécurisée et d'opérer avec une absence d'autorité centrale, grâce à la mise en œuvre d'un protocole informatique de validation décentralisée. Elle repose sur une base de données distribuée à grande échelle, où les données se rassemblent en blocs. Ces derniers renferment en leur sein l'empreinte numérique cryptographique du bloc précédent, formant ainsi une chaîne et un registre infalsifiable dont l'interconnexion est garantie par des mécanismes de sécurité cryptographique.



1. Transaction de A vers B
2. Transaction inscrite dans un bloc
3. Le bloc est validé par le réseau grâce à des techniques cryptographiques
4. Le bloc validé est ajouté à la chaîne de blocs (blockchain)
5. B reçoit la transaction de A

Ce dispositif de consensus se révèle crucial pour préserver l'intégrité des données, obligeant les participants du réseau à valider chaque nouveau bloc en accord avec des paramètres prédéfinis, préalablement à son ajout à la chaîne. Cette architecture décentralisée, jumelée à des protocoles cryptographiques, parmi lesquels des systèmes de clés asymétriques, des fonctions de hachage et des mécanismes de consensus, confère à la blockchain une robustesse singulière, la rendant difficile à pirater ou corrompre.

Les "tokens", se définissent comme des actifs numériques érigés sur une blockchain existante, suivant des normes préétablies (telles que les ERC-20 sur Ethereum). La "tokenisation" dans ce cadre consiste à représenter des actifs du monde réel en tokens, ou jetons, inscrits sur une blockchain, qu'elle soit publique ou privée. La propriété des actifs est garantie par la possession des clés cryptographiques associées aux tokens, transférables de manière sécurisée.

Etat des lieux de la blockchain en France

Les actifs numériques pour les paiements B2C au quotidien

L'intérêt croissant du grand public pour les actifs numériques ne semble pas se démentir. Une étude KPMG pour l'Association des Actifs Numériques (ADAN) note ainsi que près d'un Français sur dix possède des cryptos, et plus d'un quart pourrait en faire l'acquisition dans les années qui viennent[2].

Néanmoins, l'usage d'actifs numériques comme actif de règlement demeure aujourd'hui encore assez limité. Une étude de CSA Research note que 19 % des Français déclarent être prêts à payer en cryptoactifs, quand seuls 5 % des participants au sondage indiquent avoir déjà réalisé des achats avec des cryptomonnaies[3].

Des solutions émergent néanmoins pour faciliter l'utilisation de ces actifs en essayant de rendre leur utilisation aussi simple qu'une carte bancaire. A titre d'exemple, Mastercard propose des programmes permettant aux acteurs natifs de la crypto de délivrer des cartes aux consommateurs, offrant la possibilité de dépenser leurs actifs numériques partout où le réseau Mastercard est accepté. Personne dans la chaîne de valeur, à l'exception du prestataire

[1] Statista, (2023), *Répartition des ventes en ligne de produits selon la part des moyens de paiement utilisés en France en 2023.* Disponible sur: https://fr.statista.com/statistiques/504994/modes-de-paiement-les-plus-utilises-ecommerce-france/

[2] KPMG / ADAN. (2023). *Web3 et Crypto en France et en Europe : Adoption par le grand public et applications par les industries.*
[3] CSA / EKINO / EY / GLOBAL P.O.S / SMARTCHAIN. (2020). *Les Français et les nouveaux moyens de paiement.*

de services crypto agréé, n'a accès aux actifs numériques, et le commerçant est payé en monnaie fiat. À la suite de la demande d'autorisation de la carte, une quantité appropriée d'actifs numériques est convertie en monnaie fiat sur l'exchange crypto. Mastercard, l'acquéreur et le commerçant ne traitent que de la monnaie fiat, mais le consommateur a lui payé en crypto pour ses achats du quotidien.

Du côté des commerçants, la startup française Lyzi note que les freins évoqués par de nombreuses entreprises sont **l'importante volatilité des actifs, le manque de garantie du chiffre d'affaires encaissé et la difficulté de déploiement.** De nombreux cas d'usages retail sont récemment apparus, permettant une utilisation plus répandue par les consommateurs et l'exploration de moyens alternatifs tels que les cartes cadeaux crypto par exemple. C'est le cas de plusieurs centres commerciaux de la foncière Apsys qui, après une expérimentation lancée à Beaugrenelle à Paris, ont décidé de le généraliser à l'ensemble de leurs centres commerciaux français. On constate cependant que la plupart des commerçants enclins à accepter le paiement en crypto souhaitent réduire leur exposition en ne portant pas directement ces dernières dans leur comptabilité et privilégient donc les acteurs proposant des réversions en monnaie fiat sur leur compte. C'est à cette problématique que répond notamment Lyzi.

> *« Quiconque veut utiliser de la crypto doit pouvoir le faire de manière aussi facile que d'utiliser sa carte de crédit ou débit. C'est dans ce contexte que Mastercard souhaite développer des solutions, élargir sa gamme de produits pour répondre aux choix des consommateurs et des entreprises qui ont décidé de bénéficier et de naviguer dans ce secteur. Finalement, quelle que soit la manière dont une personne veut payer, elle aura toujours besoin d'un partenaire de confiance pour sécuriser le paiement et établir des règles claires en cas de litiges. »*
>
> **VALÉRIE NOWAK**, MASTERCARD

Selon Catherine Philippe, associée Blockchain & cryptoactifs chez **KPMG France**, cette situation s'explique par le fait que les outils de paiement traditionnels sont déjà efficaces, limitant l'incitation des commerçants à ajouter d'autres moyens de paiement, à moins de vouloir montrer leur appartenance à cette « communauté ».

Vers la création de réseau pour les actifs numériques – L'exemple du Multi Token Network

Avec son approche multi-rails, Mastercard a pour objectif d'offrir un large choix aux consommateurs et aux commerçants. Cela inclut un travail approfondi pour faciliter l'utilisation des actifs numériques au quotidien. C'est dans cet esprit que Mastercard a lancé en 2023 le développement du Multi-Token Network™ (MTN). Le MTN fournit un ensemble de capacités conçues pour rendre les transactions au sein des écosystèmes d'actifs numériques et de blockchain plus sécurisées, évolutives et interopérables. L'objectif final est d'offrir des applications de paiement et de commerce plus efficaces. Le MTN vise à libérer le potentiel des écosystèmes d'actifs numériques en atténuant certains de leurs risques les plus importants.

Les actifs numériques dans le secteur bancaire (selon Deloitte et Banking Circle)

On constate aujourd'hui un intérêt croissant pour la technologie blockchain et les acteurs de la finance traditionnelle y accordent une plus grande attention. Pour avoir un aperçu de l'avenir de la blockchain dans le domaine des paiements, nous devons d'abord comprendre certaines limites de l'infrastructure actuelle :

- Les paiements transfrontaliers restent difficiles avec l'implication de nombreux intermédiaires ;
- Le règlement en temps réel demeure un problème avec des délais les weekends et jour fériés ;
- Près d'1,4 milliard d'adultes restent éloignés du monde bancaire, créant des problèmes d'accessibilité.

La technologie blockchain offre des solutions potentielles à ces difficultés.

1. La blockchain peut fournir **un système de règlement en temps réel**, permettant l'échange simultané d'actifs de façon instantanée. Les prestataires de services de paiement (PSP) et les banques n'ont plus besoin de préfinancer des comptes auprès de diverses banques correspondantes pour faciliter ces paiements.
2. **L'argent programmable** change également la donne. L'un de ces cas d'essai est le projet Orchid de l'Autorité monétaire de Singapour, qui l'a mis en œuvre sous la forme d'un code de contrat intelligent spécifiant les conditions dans lesquelles une monnaie numérique sous-jacente peut être utilisée.
3. Les **stablecoins** constituent une innovation à fort potentiel, mais doivent encore faire leurs preuves en matière de fiabilité et gagner la confiance des régulateurs pour jouer un rôle significatif dans l'économie :
   - **Stabilité de la valeur** : leur volatilité est moindre que celle des cryptomonnaies traditionnelles comme le Bitcoin, les rendant plus adaptés comme moyen de paiement.
   - **Vitesse et faibles frais de transaction** : à l'instar de toutes cryptomonnaies les transactions sont rapides et peu coûteuses.
   - **Accessibilité** : ils offrent une entrée simple vers l'univers crypto pour les néophytes.
4. La **transparence** est renforcée grâce aux explorateurs de blockchain et aux outils de filtrage on chain. Lorsque l'argent tokenisé est utilisé dans les transactions, cela réduira l'utilisation de la blockchain pour le blanchiment d'argent ou le financement du terrorisme en raison de la transparence et de l'immuabilité de la blockchain.

Défis liés au développement des actifs numériques

Au cours des travaux sur le sujet, il est apparu très clairement que certains obstacles persistent pour permettre le développement des actifs numériques. Banking Circle souligne ainsi la nécessité **d'un cadre juridique clair et de lignes directrices solides sur les stablecoins et les cryptoactifs pour un meilleur accès et une meilleure participation**. La France, par l'intermédiaire de l'ACPR (Autorité de Contrôle Prudentiel et de Résolution), adresse ces sujets avec intérêt avec la publication d'un résumé de ses consultations publiques sur un cadre réglementaire pour la DeFi recommandant :

- La mise en place des mesures relatives à la fiabilité des infrastructures blockchain sur lesquelles la DeFi – ou d'autres formes de finance tokenisée – peuvent se développer ;
- L'élaboration de règles adaptées à la nature et au fonctionnement des contrats intelligents ;
- La définition d'une gouvernance assurant une protection adéquate des clients DeFi.

Deloitte note également que les **stablecoins rencontrent eux aussi certains défis qui devront être résolus :**

- Risque pour la souveraineté monétaire des États en cas d'adoption massive.
- Risque de fuite en cas de crise et d'effondrement de leur réserve de valeur.
- Opacité des mécanismes de stabilisation et audits insuffisants.
- Cadre réglementaire encore approximatifs.

Leur intégration dans le système de paiement français demeure incertaine, mais des actions sont en cours pour encadrer ces évolutions. La Direction générale du Trésor se concentre notamment sur leur encadrement réglementaire pour garantir la stabilité financière, en exigeant par exemple des réserves liquides et convertibles en monnaie fiat.

La France, hub européen des actifs numériques ?

D'abord suspicieuse face à cette nouvelle catégorie d'actifs, la position des autorités françaises a depuis évolué en cherchant à établir un équilibre entre innovation et encadrement du secteur tout en cherchant à positionner la France comme un fer de lance des actifs numériques. L'ancien ministre délégué chargé de la transition numérique et des télécommunications, Jean-Noël Barrot, a ainsi régulièrement exprimé la volonté du gouvernement de faire de la France un véritable "hub" pour les cryptos. Comme l'a rappelé Bastien Lafon lors de la table ronde du 12 septembre 2023, ce « hub crypto » est un contrat de confiance entre le secteur privé et les autorités pour faciliter la communication et la compréhension des besoins industriels.

Cet encadrement passe notamment par la réglementation MiCA. Ce règlement européen sur les marchés de cryptoactifs vise à créer un **système réglementaire harmonisé au niveau de l'Union européenne** pour le fonctionnement des marchés des cryptoactifs. Il aligne la directive sur les services de paiement (PSD) avec ces nouvelles technologies, et s'assure que ces marchés fonctionnent correctement tout en garantissant les droits des consommateurs et des investisseurs, l'équité du marché et la stabilité financière.

Pour son application, la France semble être pionnière en permettant aux acteurs de collaborer étroitement avec les autorités concernées, telles que la Direction générale du Trésor, la Banque de France, l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF). Bastien Lafon rappelle ainsi la double stratégie de la France : « *favoriser l'innovation tout en protégeant le consommateur* », ainsi que la volonté du Trésor de s'assurer que « *la directive sur les services de paiement et MiCA s'intègrent de manière harmonieuse* ». Il souligne également que le Trésor encourage les acteurs publics, notamment la Banque de France et la Banque centrale européenne, à explorer les opportunités offertes par la blockchain, notamment en ce qui concerne les monnaies numériques de banque centrale (MNBC) et les différentes opportunités qu'elles pourraient apporter.

> *« Le temps où les autorités politiques et les superviseurs observaient avec interrogation le secteur des cryptos est un moment vraiment révolu, ce qui est bienvenu. Nous pensons par ailleurs que la création d'un euro numérique peut remplir un certain nombre d'objectifs de structuration du secteur des paiements, une sorte de nouvelle étape pour aider à l'intégration européenne, pour favoriser la souveraineté en matière de paiements et pour assurer un ancrage monétaire comme le rappelle régulièrement la BCE ».*
>
> **BASTIEN LAFON**, DIRECTION GÉNÉRALE DU TRÉSOR

Un pas dans la bonne direction, bien que Faustine Fleuret rappelle pour l'Adan le besoin « *d'identifier entre ces réglementations françaises et européennes des règles très similaires où le pont peut être fait afin de faciliter le travail des acteurs et des régulateurs. […] Opérationnellement, il reste donc encore beaucoup de choses à faire afin que la transposition de MiCA, en France, et la mise en application dans toute l'Europe soit la plus fluide et efficace possible.* »

Vers une hybridation des infrastructures de paiement pour répondre aux attentes des consommateurs

Malgré l'engouement suscité par les actifs numériques ces dernières années, leur intégration au sein des transactions quotidiennes reste limitée du fait de défis persistants. Elle demeure encore cantonnée à certains usages de niche et les modes de paiement traditionnels comme les espèces et les paiements par carte devraient rester la norme dans les années à venir.

Néanmoins, la démocratisation des actifs numériques paraît probable à long terme. Les actifs numériques et leur technologie sous-jacente basée sur la blockchain pourraient ainsi connaître un développement majeur similaire à celui d'Internet, en permettant de résoudre certains défis que rencontrent les systèmes de paiement traditionnels.

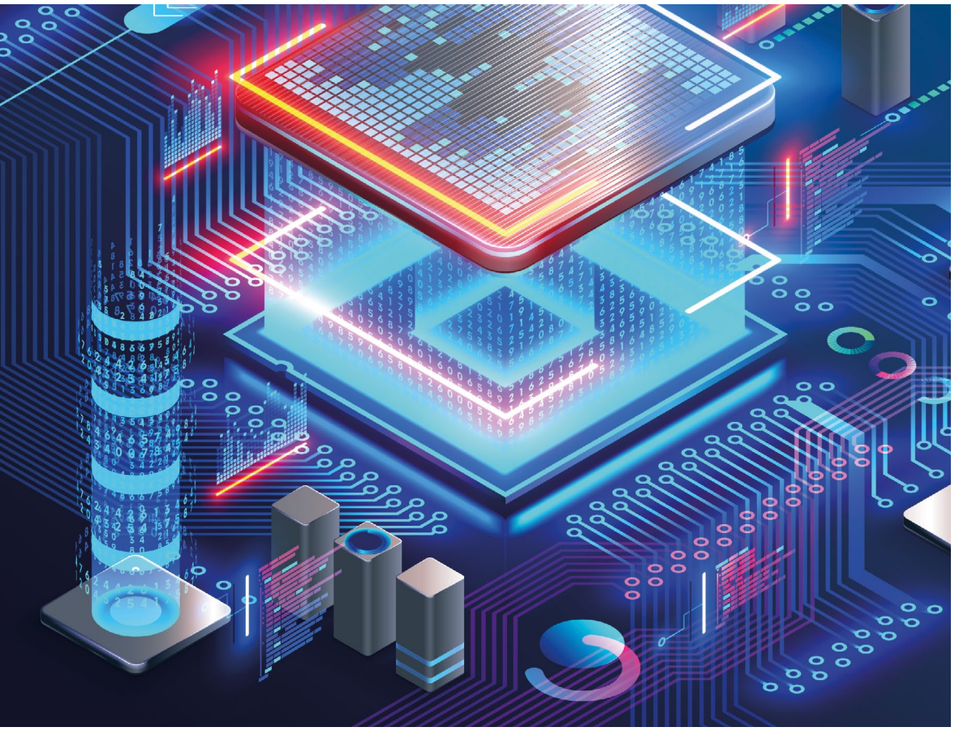
En 2030, l'utilisation de la blockchain dans les paiements en France pourrait ainsi aboutir à une architecture hybride, caractérisée par une convergence des acteurs et des technologies tout en apportant le « meilleur des deux mondes ». Cette architecture hybride favoriserait l'innovation tout en assurant une réglementation appropriée pour garantir la stabilité financière et la protection des consommateurs. Les consommateurs et les commerçants pourraient bénéficier de la facilité d'utilisation et de la sécurité des cartes bancaires tout en profitant des avantages de la blockchain :

- Des transferts internationaux quasi-instantanés réduisant les délais ;
- Des transactions enregistrées dans la blockchain offrant une transparence renforcée ;
- Des contrats intelligents automatisant les paiements basés sur des conditions prédéfinies ;
- Des technologies de confidentialité garantissant la sécurité des données personnelles.

En fin de compte, les paiements continueront à se résumer à une question de choix pour les utilisateurs, avec des modes de paiement se complétant en fonction des cas d'usage recherchés. La priorité semble être d'assurer une interopérabilité entre ces modes de paiement pour permettre de répondre aux différents cas d'usage sans pour autant augmenter les frictions pour les utilisateurs.

Dans ce contexte, la France a la possibilité de se positionner comme un acteur central au sein de l'UE, prête à jouer un rôle essentiel dans la promotion et l'adoption de solutions basées sur la blockchain dans le domaine des paiements. Cette évolution est encouragée par le gouvernement français qui incite au développement de cette technologie qui se positionne comme fer de lance de la mise en œuvre d'un cadre réglementaire clair et stable.

Les échanges à venir sur MiCA 2 seront à n'en pas douter une nouvelle étape dans l'institutionnalisation des actifs numériques, voie nécessaire pour aboutir à une tokenisation du commerce.



Moyens de paiement – Le paiement à la fois invisible et omniprésent

La carte bancaire, outil incontournable du commerce

Aujourd'hui, le moyen de paiement préféré des Français reste sans conteste la carte bancaire. En France, plus de 60 % de la consommation courante est réglée avec une carte bancaire, selon la Banque de France. Ce sont près de 29,5 milliards de transactions qui ont été effectuées, en 2022, dont 62 % par carte bancaire. Cela correspond à une augmentation de 14 points par rapport à 2012. La pandémie de Covid-19 aura également entrainé l'essor du paiement sans-contact dont le plafond a été rehaussé à 50€. Sur l'année 2022, les chiffres de la Banque de France montrent que 60 % des paiements par carte bancaire ont été réalisés en sans-contact[4].

Depuis quelques années, nous observons l'émergence de nouveaux supports de paiement qui s'inscrivent, en partie, dans le cadre du développement de l'Internet des objets (IoT). C'est notamment le cas du paiement par mobile, par bague ou encore par montre connectée qui s'accompagnent de l'entrée des Big Tech dans le secteur.

Au regard du développement exponentiel de l'IoT, nous pouvons nous attendre à ce que le « *paiement soit invisible, devenant une fonctionnalité des objets plutôt qu'une transaction en tant que telle* »[5]. Les Français devront néanmoins s'emparer de ces fonctionnalités alors même que le paiement par carte physique est devenu une habitude bien ancrée.

Des paiements de plus en plus numériques et dématérialisés avec la montée en puissance de l'IoT

D'après GSMA Intelligence, le nombre d'appareils connectés dans le monde devait s'élever à 19 milliards en 2023 et devrait approcher les 26 milliards d'ici à 2026. Rien qu'en France, environ 700 millions de connexions à l'IoT seront établies en 2026, soit environ dix appareils IoT pour chaque Français[6].

Comme le souligne G+D, l'IoT consiste ainsi à interconnecter ces "objets" physiques et numériques grâce aux technologies de l'information et de la communication, permettant d'offrir des services avancés. Les appareils physiques équipés de modules de connectivité peuvent fournir un flux de données constant permettant d'obtenir des informations en temps réel et de nombreux cas d'usages comme la maintenance prédictive et à distance des machines. À l'avenir, cela pourrait être le paiement autonome où les machines et les appareils se paient mutuellement après l'accomplissement d'un certain type d'activité, comme le paiement au résultat ou le pay-per-use.

Andréa Toucinho confirme cette tendance lors de la table ronde du 16 novembre 2023, en rappelant qu'en France, selon le baromètre annuel CB/Kantar, en 2022, 25 % des consommateurs

[4] Banque de France. (2023). *Bulletin de la Banque de France 249/4 - Novembre-Décembre 2023.*
[5] Nicola Bates, President and CEO Siemens Capital, Payments Unbound, Volume 4 – Ready Player One, The Gaming economy levels up. J.P.Morgan Payments & Wired p.46
[6] ABI Research. (2023). *IoT Market Tracker - Worldwide.*

utilisent déjà le paiement mobile et 25 % se disent prêts à l'adopter. L'avènement de la 5G, avec sa capacité à connecter des milliards d'appareils, amènera inévitablement un changement significatif chez les consommateurs. Ces évolutions conduiront à leur tour à l'émergence de nouveaux produits et services innovants. Ces tendances influenceront et modifieront la manière dont les particuliers et les entreprises effectuent leurs paiements.

Faire de chaque objet du quotidien un outil de paiement

Pour Barbara Sessa, Senior Vice President, Head of Consumer Products chez Mastercard, chaque appareil connecté devient un moyen de commerce. Deux cas d'usage significatifs ont ainsi été mis en avant :

- **Dans les Magasins** : En Europe, les consommateurs ont massivement adopté le paiement avec leur Mastercard via des portefeuilles numériques, tels que Apple Pay, Google Pay ou Samsung Pay, et un nombre toujours croissant utilisent leurs objets connectés préférés, comme des bagues de paiement, bracelets, traqueurs de fitness ou montres, pour effectuer des paiements sans contact. Ces dispositifs portables, sécurisés et discrets, offrent un nouveau moyen de paiement, différent de la carte plastique traditionnelle, bien que les infrastructures de paiement restent les mêmes. Barbara Sessa observe que l'Europe est à l'avant-garde de la tendance mondiale à l'adoption des paiements sans contact via des dispositifs portables. De plus, elle note qu'il y a une tendance notable parmi les jeunes, qui s'attendent de plus en plus à utiliser divers moyens de paiement au-delà des cartes traditionnelles.
- **Innovations dans les paiements en ligne et embarqués dans les véhicules** : Un partenariat avec Mercedes-Benz a permis aux conducteurs de payer leur carburant sans quitter leur véhicule, en utilisant une authentification biométrique sécurisée. D'ici 2030, on s'attend à ce que plus de 600 millions de véhicules dans le monde disposent de fonctionnalités similaires. La croissance de l'Internet des objets (IoT) et les efforts des pouvoirs publics dans le développement de "villes intelligentes" sont susceptibles d'élargir l'utilisation de ces technologies.

« Les deux gros éléments liés au paiement sont la tokenisation réseau, pour être sûr que dans l'objet ne soit pas stocké, entre autres, le vrai numéro de la carte et qu'il soit bien sécurisé dans un secure element, comme on trouve dans les smartphones. Et puis, au moment du paiement, c'est l'authentification, avec la reconnaissance biométrique. Là aussi, on a les solutions pour aider et sécuriser de bout en bout afin de limiter les problèmes de confiance. »

FRANÇOIS POILBOUT, THALES DIS

Paiement Mobile

Des appareils IoT, tels que les smartphones, les montres intelligentes et les bracelets connectés, sont utilisés pour effectuer des paiements sans contact à l'aide de technologies comme la communication en champ proche (NFC).

Objets Connectés dans le Commerce

Des dispositifs tels que les terminaux de paiement intelligents, les écrans de point de vente (PDV) interactifs et les distributeurs automatiques connectés permettent des transactions simplifiées.

Véhicules Connectés

Les voitures connectées peuvent être équipées de systèmes de paiement embarqués pour faciliter le règlement des péages, des parkings, et d'autres services liés à la conduite.

Paiements dans l'Écosystème Domestique

Les objets connectés dans la maison, tels que les réfrigérateurs intelligents et les assistants personnels, peuvent être équipés de fonctionnalités de paiement pour la commande automatique de produits.

Wearables

Les dispositifs portables tels que les montres intelligentes, les anneaux connectés et les lunettes intelligentes peuvent faciliter les paiements en offrant des fonctionnalités sans contact.

Commerce Connecté

Des environnements de vente au détail intelligents utilisent des dispositifs IoT pour permettre des paiements automatisés, par exemple, en détectant automatiquement les articles pris d'une étagère et en débitant le compte du client. (Amazon Go)

La tokenisation est essentielle pour intégrer les systèmes de paiement dans les appareils connectés, en assurant des transactions sécurisées et transparentes sur diverses plateformes et technologies. Dix ans après le lancement de sa technologie de tokenisation, Mastercard traite désormais chaque semaine un milliard de transactions de ce type et a annoncé récemment son objectif de tokeniser l'ensemble des transactions e-commerce, en Europe, à l'horizon 2030.

De son côté, Thales intervient dans différentes verticales, dont la santé connectée, les compteurs connectés, et surtout l'automobile, explique François Poilbout, Automotive Business Director chez Thales. Avec l'IoT, les opportunités dans le secteur de la mobilité se multiplient, allant des infrastructures routières, du paiement des parkings, des péages, des bornes de recharge électriques à l'achat d'options dans les véhicules. Les perspectives et possibilités d'une voiture capable de réaliser des paiements autonomes sont nombreuses et faciliteraient la vie du conducteur, mais les questions de sécurité et d'authentification restent au cœur de ces évolutions. Aujourd'hui dans l'IoT, Thales développe principalement des solutions de connectivité et de cybersécurité.

Quels bénéfices pour l'IoT dans les paiements ?

G+D note qu'avec les progrès constants de l'automatisation, donner aux dispositifs IoT la capacité d'effectuer des transactions commerciales de manière autonome apparaît comme la prochaine étape. Mais cette vision est étroitement liée aux avantages qui en sont attendus.

La première motivation est la **commodité**. Si un appareil IoT peut identifier une demande et déclencher automatiquement la satisfaction de cette demande, cela élimine les processus

> *« Je pense que l'enjeu est de construire ensemble des process dignes de confiance. Les parcours physiques et numériques des consommateurs convergent dans les domaines de la banque, du commerce et des paiements et Il y a principalement trois piliers technologiques concernés : la connectivité, l'identité et le paiement. Il faut que ces actifs soient consolidés et qu'il y ait des passerelles d'interconnexions sécurisées. La confiance doit évoluer en même temps que ces parcours et ensemble nous devons trouver un équilibre entre la sécurité et la commodité, sans accroître la complexité des transactions quotidiennes. Cela stimule l'innovation dans toutes les formes de services bancaires et de paiements et c'est pour ça que les pilotes sont extrêmement importants. En tant qu'industriels, nous avons une responsabilité à proposer des solutions souveraines et sécurisées prenant en compte les attentes des consommateurs comme celles de toutes les parties concernées. Il en va d'un marché à fort potentiel et d'un confort supplémentaire au quotidien pour nos concitoyens et nos commerçants »*
>
> **PHILIPPE DELANOUE**, G+D

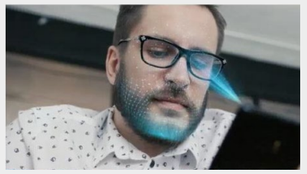
manuels entraînant une plus grande fluidité et un gain de temps pour l'utilisateur. Les cas d'usage B2C devraient être le véritable moteur de l'adoption. On pourrait par exemple imaginer des appareils tels que des réfrigérateurs planifiant par eux-mêmes leur propre (ré) approvisionnement. L'ergonomie et la fluidité du parcours sont ainsi essentielles pour séduire les consommateurs et se diriger vers une plus grande acceptation.

La deuxième motivation fondamentale est la **fiabilité**. Si l'appareil IoT est capable d'effectuer certaines transactions automatiquement, cela peut contribuer à garantir une performance optimale et ininterrompue de l'appareil.

La troisième concerne **l'amélioration de l'efficacité, l'optimisation des coûts et la valeur commerciale possible.** En faisant en sorte que les dispositifs IoT effectuent des transactions de manière autonome, les processus connexes à ces transactions seront également automatisés. Une fois ce stade atteint, ces processus comprendront la reconnaissance de la demande, l'évaluation des fournisseurs potentiels, la mise en service, l'accord sur les conditions, la vérification du service/bien fourni et le paiement, y compris les fonctions comptables telles que la facturation et la taxation. Les appareil IoT avec ce niveau d'autonomie seront conçus pour exécuter ces tâches de manière optimisée et permettront ainsi une meilleure efficacité et une réduction des coûts tout en éliminant les processus manuels.

Le corps humain, dernière frontière pour le paiement ?

Et si le corps humain devenait le medium ultime pour réaliser ses paiements au quotidien ? Avec le développement de la biométrie comme outil d'authentification, cette possibilité devient de plus en plus une réalité.



Reconnaissance faciale
Forme d'authentification biométrique qui est devenue de plus en plus populaire, avec l'essor de solutions telles que WorldCoin. Cette méthode offre un niveau de sécurité élevé en raison du caractère unique des motifs de l'iris de chaque personne. Sa praticabilité est parfois entravée par la résistance de l'utilisateur et les difficultés de lisibilité

Reconnaissance du sourire

Reconnaissance des empreintes digitales

Reconnaissance de l'iris ou de la rétine
Méthode d'authentification populaire. Cependant, elle n'est pas sans poser quelques problèmes. Son inconvénient réside dans sa vulnérabilité aux "deepfakes" pour un accès non autorisé, ce qui pose des problèmes de sécurité globale.

Selon IDEX Biometrics, la biométrie offre une myriade de possibilités allant des paiements à la gestion de l'identité. La biométrie améliore considérablement l'expérience consommateur et des commerçants en permettant un paiement invisible et sans couture.

En plus d'une expérience client sans friction, l'amélioration de la sécurité est un facteur majeur dans la prise en compte de la technologie biométrique. A titre d'exemple, les cartes biométriques, intégrant un capteur d'empreintes digitales dans une carte de paiement sans contact, sont dotées d'algorithmes et de capacités de cryptage permettant de détecter et de répondre aux attaques frauduleuses. L'empreinte digitale cryptée de l'utilisateur enregistrée sur une carte biométrique ne peut pas non plus être copiée. Lors de l'enregistrement, une représentation numérique abstraite de l'empreinte digitale est stockée et cryptée dans l'élément sécurisé de la carte, qu'il est impossible de reconstituer et à partir de laquelle il est impossible de créer une image.

En septembre 2021, le **Crédit Agricole** a déployé à grande échelle une carte bancaire capable de reconnaître l'empreinte digitale du porteur. Lors de la table ronde, Xavier Vaslin nous explique notamment les défis techniques que représentaient cette carte en sans contact et avec un capteur biométrique. Le facteur d'authentification est alors directement porté

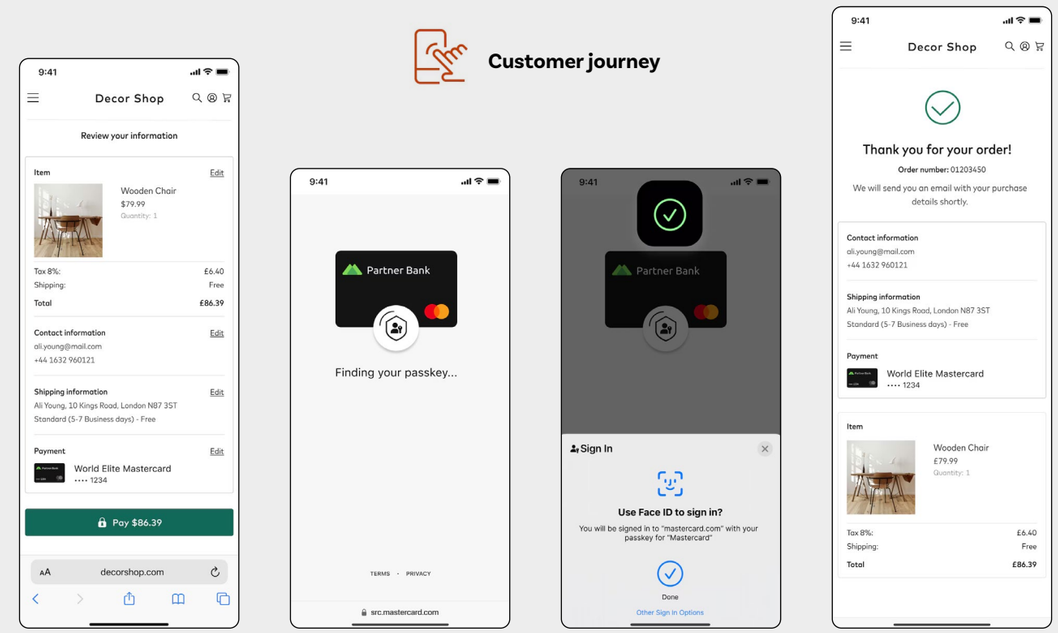
> *« Nous sommes très attentifs à la convergence de l'authentification du paiement avec l'identification du payeur. Il y a un certain nombre de projets européens, sur l'identité numérique, et à partir du moment où vous embarquez un certain nombre d'attributs de cette identité, dont un moyen de paiement, vous allez pouvoir renforcer le lien entre un payeur et son moyen de paiement. Il y a encore un certain nombre d'éléments réglementaires, ou en tout cas de standardisation à mener pour assurer des parcours fluides. »*
>
> **BERTRAND PINEAU**, MERCATEL

par le moyen de paiement, de la même manière que pour les paiements mobiles actuels. Aujourd'hui, la carte biométrique fait encore face à des défis techniques, notamment autours de l'efficacité du capteur comme cela a pu être le cas avec les paiements mobiles.

Néanmoins, l'élimination du mot de passe ou du code PIN crée instantanément une expérience utilisateur plus fluide. En moyenne les utilisateurs gèrent 100 mots de passe différents pour divers comptes et abonnements. Les personnes malvoyantes sont également frustrées de devoir franchir les barrières sensorielles des codes PIN, amenant parfois à l'abandon d'une transaction par crainte de rencontrer une difficulté ou de faire face à un vol de mot de passe. L'authentification biométrique permet aux utilisateurs d'appuyer simplement sur leur carte à puce biométrique ou de scanner leur visage pour effectuer une transaction, ce qui rend l'expérience de paiement plus rapide et plus fluide.

Dans cette même dynamique, plusieurs entreprises proposent désormais l'utilisation de passkeys couplées à de la biométrie comme méthode d'authentification. S'appuyant sur les normes de l'alliance FIDO, les passkeys « *remplacent les mots de passe qui permettent une connexion plus rapide, plus facile et plus sécurisée aux sites Web et aux applications sur les appareils d'un utilisateur. Contrairement aux mots de passe, les passkeys sont toujours solides et résistants au phishing* »[7]. Le processus d'authentification via les passkeys est en moyenne 40% plus rapide qu'une authentification utilisant un mot de passe classique. Ce type de solutions d'authentification commence à se répandre comme illustré par la récente annonce de Mastercard de remplacer les métuodes traditionnelles d'authentification comme les mots de passe et les SMS OTP par des passkeys couplés à un scan biométrique.

[7] FIDO alliance – Passkeys 101 - https://fidoalliance.org/passkeys/



Face ID® and the Apple-owned graphic symbols depicted in the UX screen are trademarks of Apple Inc

Pour les paiements en ligne, **la biométrie comportementale** offre également de nombreux avantages, permettant des actions de **validation de manière silencieuse**, sans que l'utilisateur en ait conscience, telle que la confirmation d'opérations sensibles. Bien que cette technologie ne soit pas encore utilisée pour les paiements en France, elle se présente comme une technologie d'avenir grâce à son haut niveau de sécurité. Imaginons qu'un fraudeur veuille avoir accès à vos comptes sensibles. Même s'il parvient à obtenir votre nom et votre mot de passe, il ne pourra jamais reproduire votre comportement.

La sécurité des données, pré-condition au succès de la biométrie

Les questions prédominantes autour de la biométrie concernent la sécurité des données des consommateurs. Il est donc impératif de fournir une transparence totale pour rassurer les utilisateurs quant à l'enregistrement sécurisé de leurs marqueurs biologiques dans un secure-

element non accessible. Xavier Vaslin du Crédit Agricole rappelle notamment qu'*« en France, on travaille vraiment sur de la biométrie stockée en local, dans un composant hyper sécurisé. Nous n'avons pas de base de données avec de la biométrie des personnes. On reste vraiment sur le device de la personne, qu'elle a en main, à l'instant t. Le but, d'un point de vue réglementaire, est d'éviter d'avoir à stocker quelque part une base à la fois bancaire et de biométrie. ».*

Oleg Makhotin d'IDEMIA, a souligné lors de la table ronde du 16 novembre 2023 que nos photos qui peuvent être considérées dans une certaine mesure comme des données biométriques sont partout sur Internet, par exemple dans les plateformes de médias sociaux, parfois associés avec nos données personnelles. Cependant, dans la biométrie, tout comme le cryptogramme sur une carte EMV, des éléments dynamiques sont utilisés pour renforcer la sécurité. Il souligne l'utilisation d'algorithmes spécifiques dans la biométrie comportementale, prenant en compte la dynamique inhérente à la vie humaine. L'analyse ne se limite ainsi pas à la simple apparence. Même si l'on peut partager une photo, cela ne signifie pas que n'importe qui peut l'utiliser pour effectuer des paiements. Bien que les données biométriques soient immuables, des avancées technologiques, notamment dans la biométrie comportementale, permettent ainsi une sécurisation robuste en intégrant des éléments dynamiques. *« Le rôle d'un réseau comme Mastercard c'est avant tout d'assurer la sécurité des paiements, des données et des utilisateurs de bout en bout »* note ainsi Thomas Guillerault, Director, Products & Sales, Cyber and Intelligence Solutions, Western Europe chez Mastercard.

Dans l'UE, les données biométriques sont également incluses dans le règlement général sur la protection des données (RGPD), le principal texte européen en matière de protection des données et de respect de la vie privée dans l'UE. Les données biométriques y sont définies comme des *« données à caractère personnel résultant d'un traitement technique spécifique relatif aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification unique de cette personne physique, telles que des images faciales ou des données dactyloscopiques. »* (Art. 4.14)

Perspectives pour l'utilisation de l'IoT dans les paiements

L'internet des objets incarne le fruit de la constante évolution de la technologie et des paiements. Treezor note ainsi que l'IoT va non seulement révolutionner notre vie quotidienne, mais possède également le potentiel de remodeler la façon dont nous effectuons les transactions financières. Ceci dessine un avenir où les appareils connectés, comme les véhicules autonomes, initieront, autoriseront et réaliseront des transactions financières sans intervention humaine.

Alors que nous nous dirigeons vers des paiements autonomes, il conviendra de bien intégrer ces avancées technologiques et d'adapter les mesures de sécurité et de confidentialité pour protéger les données utilisées. Les appareils connectés dotés d'intelligence artificielle vont se démultiplier dans notre environnement, créant des méthodes et applications de paiement innovantes. Toutefois, cette vision soulève également des questions cruciales en matière d'utilisation. Les implications futures sont considérables, et l'évolution des mesures de cybersécurité et de la réglementation seront indispensables pour assurer une transition fluide.

Des paiements autonomes sont la promesse d'un avenir où les transactions financières seront à la fois omniprésentes et invisibles, ce qui donne un aperçu du potentiel de la transformation du paysage financier. Cependant, le compromis entre simplicité, sécurité et authentification sera le grand défi. Dans le cas de l'automobile par exemple, **la biométrie va jouer un rôle crucial**, bien que l'ajout d'un tel capteur, peu coûteux en soi, suscite des réticences chez certains constructeurs.

La réglementation jouera néanmoins un rôle clé pour favoriser le déploiement de ces technologiques. L'exemple de l'industrie automobile est là encore assez révélateur : une nouvelle réglementation européenne en discussion vise à rendre obligatoire la présence d'une caméra sur les véhicules homologués surveillant le conducteur, ses signes de fatigue et de distraction. L'utilisation de ce matériel pourrait faciliter considérablement l'adoption des technologies biométriques pour les paiements in-car d'ici 2030. Elle résoudra le problème lié à des méthodes d'authentification inappropriées pendant la conduite et renforcera la sécurité.

On observe ainsi une multiplication des cas d'usage liés à l'IoT et à la biométrie dans les paiements ces dernières années, et cette tendance a vocation à se poursuivre à mesure que les technologies deviennent accessibles et sont adoptées par les utilisateurs. Si les rails de paiement pourraient rester les mêmes, le paiement a ainsi vocation, d'ici 2030, à changer de support en étant à la fois toujours plus omniprésent, du fait de sa disponibilité sur l'ensemble des objets de notre quotidien, tout en étant de plus en plus invisible, fluide et sécurisé.

Confiance - Sécuriser les paiements à l'ère quantique

Le quantique dans les paiements : réalité ou science-fiction ?

Bien que l'idée d'un ordinateur quantique puisse encore apparaître pour certains comme de la science-fiction, cette technologie est de plus en plus sur le devant de la scène. Des sommes importantes sont investies à travers le monde dans cette technologie qui transcende les limites des ordinateurs classiques et ouvre ainsi la voie à des applications et innovations inédites. Pourtant, les fondements théoriques de cette révolution existent depuis plusieurs décennies. Dès 1982, Richard Feynman a établi un concept qui deviendra plus tard l'ordinateur quantique. Plus de deux décennies seront nécessaires pour que le premier dispositif expérimental apparaisse et près de 30 ans pour voir le premier ordinateur quantique opérationnel à très petite échelle.

Les ordinateurs quantiques sont les prochaines générations d'ordinateurs qui s'appuient sur des principes fondamentalement différents de ceux des ordinateurs numériques classiques. Les ordinateurs quantiques, comme leur nom l'indique, s'appuient sur les principes de la physique quantique ou de la mécanique quantique pour représenter les informations. Cela donne aux ordinateurs quantiques la possibilité de résoudre certains problèmes difficiles de manière beaucoup plus efficace qu'avec des ordinateurs numériques classiques.

Mais alors que les ordinateurs quantiques ouvrent de nouvelles frontières, l'univers des transactions financières fleurit grâce à la robustesse de la cryptographie. Chaque jour, des milliards de transactions effectuées sont assurées et protégées grâce à celle-ci. Comme l'explique G+D, la cryptographie préserve la confidentialité, l'authenticité et l'intégrité des données transmises lors d'un paiement par carte tout au long du processus, et ce en ligne comme hors ligne. Cela comprend par exemple l'échange d'informations entre la carte et le terminal, ainsi qu'entre la carte et le système hôte de l'émetteur. La cryptographie est ainsi utilisée pour sécuriser les canaux de communication entre deux parties en codant les informations d'une manière presque impossible à intercepter ou à déchiffrer par des fraudeurs.

Toutefois, ces transactions pourraient être menacées si les futurs ordinateurs quantiques avaient la capacité de casser les algorithmes cryptographiques asymétriques classiques tels que le RSA (Rivest-Shamir-Adleman Encryptions) et la cryptographie à courbe elliptique (ECC) qui sont utilisés aujourd'hui.

La sécurisation des données à l'aide d'algorithmes à sécurité quantique est donc essentielle. L'utilisation du quantique dans les paiements n'en est qu'à ses débuts, mais elle pourrait révolutionner la manière dont nous effectuons nos transactions financières en ligne. À mesure que la technologie progresse, il est probable que de plus en plus d'entreprises s'y tournent afin de sécuriser leurs systèmes de paiement et protéger les informations financières de leurs clients.

Explication du risque cryptographique

Krisztian Benyo, Ph.D. de **Pasqal** a souligné lors de la table ronde du 7 décembre 2023 que des algorithmes pouvant fonctionner efficacement sur l'ordinateur quantique, avant même qu'il ne devienne réalité, existent d'ores et déjà. L'un des exemples les plus célèbres est celui de Peter Shor, qui a conçu un algorithme de factorisation des nombres entiers en 1994, un des tout premiers algorithmes quantiques. Il s'agit d'un problème mathématique classique, complexe et difficile, qui constitue le fondement principal de la cryptographie moderne basée sur une clé publique. En effet, cette dernière repose sur le fait que, malgré des décennies de recherche, nous avons des problèmes mathématiques que nous ne savons pas résoudre. Cependant, certains problèmes deviennent de façon exponentielle plus faciles à résoudre grâce aux caractéristiques des ordinateurs quantiques.

Comme le souligne Elli Androulaki, PhD., d'**IBM Research**, « *Dans certains cas, les entreprises doivent agir immédiatement. Par exemple, lorsqu'une transaction doit avoir lieu aujourd'hui, des données sensibles doivent être échangées entre les participants. Cette communication doit être sécurisée à l'aide de nouveaux types de canaux de communication sécurisés, capables de préserver la confidentialité des données échangées et stockées aujourd'hui contre les ordinateurs quantiques de demain ; il s'agit de protéger les données confidentielles contre ce que l'on appelle les attaques « harvest now - decrypt later » (récolter maintenant - déchiffrer plus tard).* » Ce processus repose sur le **« protocole d'échange de clés »**, en s'appuyant à nouveau sur la cryptographie traditionnelle. Or, **un ordinateur quantique suffisamment puissant sera capable de casser la cryptographie à clé publique utilisée aujourd'hui.** En conséquence, une organisation malveillante munie d'un tel ordinateur aura le pouvoir d'usurper l'identité d'une personne ou d'accéder à des données confidentielles.

En outre, des pirates peuvent capturer une conversation ayant lieu aujourd'hui, conserver cette transcription et essayer de compromettre la confidentialité, lorsqu'ils seront en possession d'un ordinateur de la sorte. Ce phénomène est connu sous le nom de "Harvest now, decrypt later" et implique que les données d'aujourd'hui doivent être sécurisées par anticipation pour répondre aux menaces de demain. Bien que cela puisse poser problème dans certains domaines, le risque dans l'industrie des paiements reste relativement limité, car la durée de vie d'une transaction est courte, tant que les normes appropriées sont respectées.

CryptoNext Security voit plutôt des risques directs pour les paiements liés au vol de données bancaires, aux transactions à l'origine obscure ou encore aux perturbations des liquidités d'une institution financière. Ce dernier point a notamment fait l'objet d'une étude alarmante du Hudson Institute qui évalue à 8 % du PIB américain l'impact de la menace quantique sur le système financier si celle-ci n'est pas correctement prise en compte.

Un autre risque réside dans l'hétérogénéité des technologies quantiques. M. Benyo rappelle que de nombreux types d'ordinateurs quantiques sont en cours de développement ce qui entraine une grande variété dans l'éventail des cyber-attaques à envisager. La technologie étant encore en cours de maturation, la disponibilité d'ordinateurs quantiques reste faible limitant la possibilité de tester des clés modernes alors que la menace, elle, est très large.

Le risque est donc sérieux et doit être anticipé pour prendre en compte le temps de migration des infrastructures, et le cycle de vie des composants dans la chaîne de paiement.

> *« En tant que surveillant, nous appelons tous les acteurs de la chaîne des paiements à préparer dès maintenant leur migration. Comment ? En cartographiant leurs algorithmes, en listant et en triant par sensibilité toutes les données qui pourraient être affectées, en entreprenant des expériences de migration etc. Il nous paraît important de conduire des expérimentations au sein des entités avant que les normes ne soient établies pour développer les compétences requises et d'établir une feuille de route crédible qui soit validée à haut niveau. La bonne nouvelle est que nous ne sommes pas en retard. Nous avons encore le temps de le faire. La Banque de France a déjà conduit certaines expérimentations. Maintenant, une prise de conscience est nécessaire par l'ensemble des acteurs de la chaîne des paiements, aux niveaux national comme européen. »*
>
> **MARC-ANTOINE JAMBU**, BANQUE DE FRANCE

Anticiper la menace avec la cryptographie post-quantique

Face à ce constat, peut-on dire que nous sommes face à une catastrophe annoncée ? « *L'agilité cryptographique est bénéfique, car elle permet une transition en douceur d'un système vers son équivalent à sécurité quantique* », explique **Elli Androulaki, PhD. d'IBM Research**, qui souligne que « *la standardisation des schémas cryptographiques pour les signatures numériques et le cryptage à sécurité quantique est en cours.* »

Les efforts d'anticipation se concentrent sur la **cryptographie post-quantique (PQC)** ou cryptographie résistante au quantique. Cette cryptographie repose sur de nouveaux algorithmes résistants à l'ordinateur quantique et vise à être déployée sur les infrastructures existantes. Cependant, Pasqal met en garde contre l'idée répandue que pour réaliser la PQC, il faut un ordinateur quantique. La PQC ne consiste pas à utiliser un ordinateur quantique pour chiffrer, mais à se protéger de manière classique contre une menace quantique. En effet, il existe des méthodes classiques de cryptographie, qui sont en cours de développement et de standardisation et qui assurent la sécurité de nos données.

De manière générale, les systèmes de sécurité critiques, en cours de développement aujourd'hui, doivent tenir compte de la menace quantique de demain pour aboutir à un "état de préparation quantique". Cela se traduit par la **crypto-agilité** et la garantie de pouvoir remplacer facilement les composants par des équivalents quantiques sûrs, une fois que les normes auront été finalisées. Dr Steve Flinter, Senior Vice President Artificial Intelligence & Quantum Computing **chez Mastercard**, souligne l'importance de cette crypto-agilité, encourageant les émetteurs de cartes, les banques et tous les acteurs à se préparer en identifiant les éléments cryptographiques potentiellement vulnérables.

La Banque de France a ainsi mené plusieurs expérimentations sur le sujet, avec la mise en œuvre expérimentale en septembre 2022 « *d'une solution de sécurisation de communications par des algorithmes dits « post-quantiques », c'est-à-dire résistants à la puissance de calcul des futurs ordinateurs quantiques qui, d'ici quelques années, menacent de casser les clés utilisées par les algorithmes actuels.* » Ces travaux font dire à Marc-Antoine Jambu que « *la migration est techniquement faisable* » et que « *les principes d'hybridation et d'agilité cryptographique peuvent guider cette migration* ».

Le Crédit Mutuel et IBM ont de leur côté annoncé, en juin 2023, la création d'une Quantum Factory qui « *sera chargée de définir les grandes étapes de la phase de mise à l'échelle et de continuer à développer des cas d'usage afin de préparer l'intégration de l'informatique quantique dans les secteurs des services financiers et de l'assurance* ».

Les défis posés par la migration post-quantique

La **migration** des outils de cryptographie actuels vers des outils post-quantiques, dans un temps court d'une dizaine d'années, constitue un défi majeur. Les systèmes cryptographiques actuels n'ont pas été conçus pour être évolutifs, et des infrastructures entières doivent être remaniées.

Ce défi recouvre des enjeux de différentes natures :

- L'évolution des normes et réglementations ;
- L'innovation et les développements technologiques pour implémenter et déployer cette nouvelle cryptographie post-quantique ;
- La cohérence des déploiements et l'interopérabilité pour des systèmes et infrastructures globales.

Les organismes de normalisation tels que le NIST (National Institute of Standards and Technology) aux États-Unis et l'ANSSI travaillent au développement et à la normalisation d'un nouvel ensemble d'algorithmes dits de cryptographie post-quantique (PQC), qui seront résilients face à la menace posée par un futur ordinateur quantique puissant. Par exemple, le NIST a entamé en 2016 un processus de standardisation d'algorithmes de cryptographie post-quantique et a effectué, en 2022, une première sélection d'algorithmes à standardiser.

Lors de la discussion, Elli Androulaki, PhD, d'IBM Research, a mis l'accent sur le besoin critique d'être prêt pour le quantique et sur les défis que pose son intégration dans les systèmes existants. Elle a souligné que dans les systèmes émergents tels que les monnaies numériques des banques centrales et les tokens de dépôt, il est essentiel d'assurer la préparation quantique pour les paiements en ligne et hors ligne. En plus de la standardisation des méthodes cryptographiques, il est tout aussi important que les dispositifs des utilisateurs soient équipés de primitives résistantes aux attaques quantiques pour soutenir pleinement ces avancées.

Quelles perspectives pour le quantique dans les paiements d'ici 2030 ?

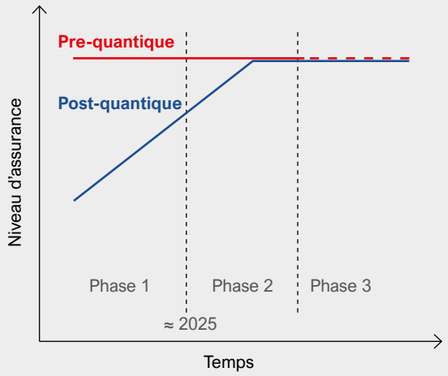
En France, l'ANSSI a défini, en avril 2022, dans un avis scientifique sa vision de la transition vers le post-quantique en 3 étapes, avec une première date pivot en 2025.

Étant donné la complexité des infrastructures de paiement et la diversité des composants sous-jacents, les défis technologiques sont variés.

- Implémentations performantes et sécurisées de ces nouveaux algorithmes de cryptographie dans des environnements contraints comme les cartes à puce.
- Malgré la faible maturité de la cryptographie post-quantique, l'implémentation hybride de protocoles conserve le niveau de sécurité existant tout en apportant une couche de sécurité à long terme résistante au quantique.
- Mise en œuvre de la crypto-agilité pour passer, là où c'est possible, d'une cryptographie rigide et figée, à une cryptographie évolutive dans la durée.

Pour chaque organisation, **l'enjeu sera de construire un plan de transition vers le post-quantique.** Pour cela, une première étape consiste à établir l'inventaire des systèmes utilisant de la cryptographie à clé publique ; et d'autre part, de lancer des expérimentations pour comprendre l'impact opérationnel de cette cryptographie post-quantique.

Certaines banques centrales, banques commerciales et fournisseurs de solutions ont lancé les premières expérimentations. Ces premiers tests sont très encourageants, mais le chantier de la cryptographie post-quantique dans les paiements ne fait que commencer.



« Chez Mastercard, nous cherchons à savoir comment nous pouvons appliquer la technologie quantique à la résolution de problèmes tels que le machine-learning, en particulier l'optimisation des algorithmes traditionnels de machine learning. Cela a évidemment des applications dans un grand nombre de domaines différents, dont la détection des fraudes. Nous étudions également les applications pour résoudre les problèmes d'optimisation. Là encore, toutes les industries sont concernées, de manière très différente. La technologie quantique va ainsi nous aider à mieux résoudre ces problèmes. »

DR STEVE FLINTER, MASTERCARD

Steve Flinter rappelle que le développement de la technologie quantique sera progressif, avec des applications à grande échelle prévues pour résoudre des problèmes commerciaux avant 2030. Mastercard collabore notamment avec D-Wave sur des problèmes d'optimisation pour conduire à des solutions commerciales basées sur ces technologies dans les prochaines années. **En matière de sécurité, Mastercard estime qu'aucun ordinateur quantique capable d'attaquer les systèmes cryptographiques ne sera disponible d'ici 2030.** Malgré cela, la mise à niveau des systèmes sera un long processus, incitant les émetteurs, les banques et d'autres acteurs à élaborer des stratégies de crypto-agilité et à remplacer progressivement les technologies obsolètes au cours des prochaines années.

Cependant, il convient également de tirer parti de cette technologie. Si les implications en matière de sécurité sont évidentes, Mastercard et de nombreux autres acteurs se concentrent également sur l'exploitation des propriétés physiques de l'univers pour nous aider à résoudre des problèmes trop complexes pour les technologies informatiques traditionnelles. Ce travail ouvre des opportunités uniques pour le secteur des paiements tels que le traitement accéléré des transactions, l'amélioration de la gestion des risques à travers une simulation plus fine de modèles financiers, l'optimisation des processus de paiement ou encore la détection de fraude avancée.

Quel potentiel pour l'IA dans les paiements ?

L'intelligence artificielle révolutionne le secteur des paiements en offrant des solutions innovantes pour améliorer l'efficacité, la sécurité et l'expérience utilisateur. À l'automne 2022, l'IA générative était principalement connue des ingénieurs en IA et des experts en mégadonnées. Aujourd'hui, elle est largement reconnue et est à l'origine d'une révolution économique. Une enquête réalisée en 2023 a montré que 55 % des PDG de grandes entreprises mondiales explorent ou testent l'IA générative.

L'un des principaux atouts de l'IA dans les paiements réside dans sa capacité à analyser de grandes quantités de données en temps réel. Avec l'apprentissage automatique et la modélisation des comportements, les banques et entreprises sont désormais en mesure de détecter plus rapidement de potentielles fraudes. Les algorithmes d'IA peuvent identifier des transactions anormales ou suspectes, en se basant sur les historiques de paiements des utilisateurs, permettant ainsi de diminuer les risques d'activités frauduleuses.

De quelle IA parle-t-on ?

Nima Sepasy indique que lorsque Mastercard réfléchit à la direction que prendront l'IA et les LLM, celles-ci peuvent être classés en trois catégories : **informée, perceptive et agentique**. Cette distinction définit la façon dont nous pouvons anticiper la transformation que l'IA apportera à la manière dont nous faisons nos achats, réservons nos voyages, naviguons dans le système de santé ou interagissons avec nos banques.[8]

L'IA informée implique l'utilisation de méthodes telles que la génération augmentée par récupération (RAG) pour augmenter les grands modèles de langage avec des types de connaissances distincts. L'objectif est de les rendre plus utiles dans des cas spécifiques, en particulier dans le secteur bancaire.

Les modèles perceptifs prennent en compte plusieurs types d'entrées, telles que des flux vidéo et des données de capteurs, afin d'apporter un niveau de conscience contextuelle aux IA. Ils rendent possibles les conversations avec des agents d'IA capables de comprendre les intentions humaines en se basant sur les expressions faciales. De plus, les modèles perceptifs peuvent intégrer les mesures et les préférences des consommateurs dans les recommandations d'achats de vêtements. Cela pourrait être particulièrement bénéfique pour les commerçants.

Pour l'IA agentique, les modèles d'IA générative acquerront la capacité de fonctionner de manière proactive, avec leur propre autonomie, en l'absence de consignes, et de fonctionner indépendamment d'un contrôle humain permanent. Ainsi, l'IA agentique pourra notamment alimenter le secteur bancaire dans des domaines tels que la planification financière automatisée et la prévention des fraudes, ainsi que les programmes de fidélité avec des offres personnalisées ou la réservation de voyages.

[8] Selon Oracle, le « *RAG fournit un moyen d'optimiser le résultat d'un LLM avec des informations ciblées, sans modifier le modèle sous-jacent lui-même ; ces informations ciblées peuvent être plus récentes que le LLM ainsi que spécifiques à une entreprise et à un secteur particuliers. Cela signifie que le système d'IA générative peut fournir des réponses contextuellement appropriées aux invités et les baser sur des données extrêmement récentes* » Plus d'informations disponibles ici: https://www.oracle.com/fr/artificial-intelligence/generative-ai/retrieval-augmented-generation-rag/

Quels cas d'usage pour l'IA générative dans la banque et les paiements ?

L'IA générative permet d'améliorer les opérations bancaires cruciales en gérant de nombreuses tâches nécessitant une quantité importante de données. En interne, les banques peuvent découvrir des informations cachées, faire des prévisions plus précises et améliorer l'efficacité du personnel. En externe, la phase des services bancaires génériques pourrait se transformer en une ère d'engagement sur mesure, où l'IA permet des expériences personnalisées. Voici quelques exemples qui peuvent être cités :

- Connaissances et réflexions[9]:

À la banque OCBC de Singapour, un outil d'IA générative transforme la manière dont les employés font des recherches, rédigent des documents et suscitent l'innovation. Les premiers essais indiquent qu'il peut réduire de moitié le temps nécessaire à la réalisation de tâches complexes.

- Technologie[10]:

Lancé fin 2023, Code Assistant for IBM Z développé par IBM est un outil de refactorisation génératif alimenté par l'IA qui convertit COBOL, le langage de programmation hérité des années 1959 encore essentiel à l'infrastructure informatique de nombreuses banques, en Java contemporain.

- Cybersécurité[11]:

SecPaLM développé par Google, un grand modèle de langage conçu pour les applications de sécurité, améliorera le Google Cloud Security AI Workbench avec des outils permettant d'identifier les codes malveillants et de répondre rapidement aux violations.

- ChatBot[12]:

Au printemps 2023, la startup Kasisto a présenté KAI-GPT, le premier grand modèle de langage spécifiquement conçu pour la banque, permettant aux chatbots bancaires d'avoir des conversations réactives de niveau humain.

- Conseil patrimonial[13]:

Morgan Stanley Wealth Management a lancé un assistant de gestion des connaissances piloté par l'IA. S'appuyant sur le ChatGPT-4 d'OpenAI, cet outil aide les conseillers de l'entreprise en leur offrant un accès direct à une collection de 100 000 documents et rapports internes.

- Marketing et communication[14]:

Le Crédit Agricole s'est associé à l'entreprise d'IA Persado pour exploiter l'IA générative dans la création d'e-mails marketing et la rédaction de textes pour les publicités Facebook et Google.

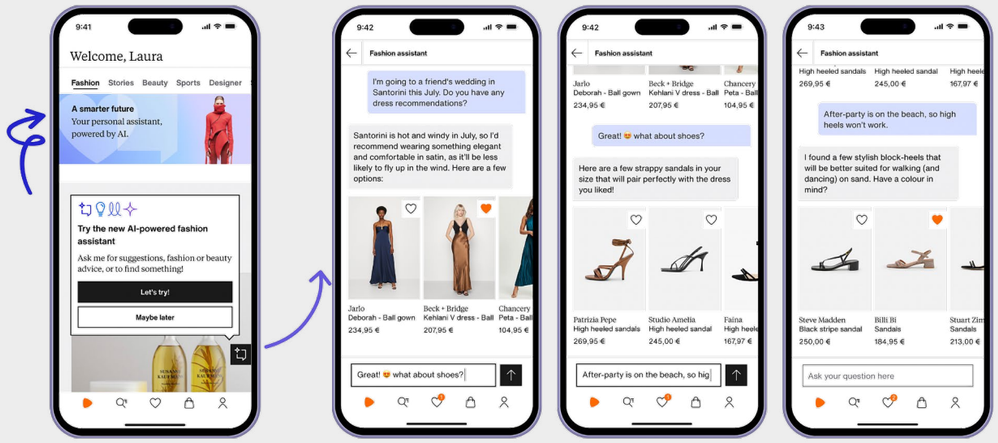
[9] OCBC: OCBC is first Singapore bank to roll out generative AI chatbot to all employees globally
[10] InfoWorld: IBM Watsonx to use generative AI to translate COBOL code into Java
[11] Google: Supercharging Security with generative AI
[12] Business Wire: Kasisto Launches KAI-GPT, the First Banking Industry-Specific Large Language Model
[13] CNBC: Morgan Stanley kicks off generative AI era on Wall Street with assistant for financial advisors
[14] Persado: Credit Agricole personalizes customer communications in an omni-channel environment

Un exemple parmi tant d'autres est la façon dont Treezor s'est associé à SAS pour mettre en œuvre une plateforme basée sur l'IA et renforcer sa lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi que la détection des risques de fraude. Cette collaboration avec SAS se traduit par un renforcement substantiel du système existant de Treezor, grâce à l'intégration d'une technologie d'IA avancée et d'une approche centrée sur les données pour améliorer de manière significative son système de suivi des transactions.

De leur côté, les commerçants peuvent améliorer l'expérience des clients grâce à une meilleure compréhension du comportement des consommateurs, en proposant un marketing plus personnalisé, en rationalisant la gestion de la chaîne d'approvisionnement en optimisant les stocks et en prédisant les tendances du marché. A titre d'exemple, Zalando annonçait dès avril 2023 le lancement d'une première version beta d'un assistant géré par ChatGPT, avec comme objectif de « *permettre aux clients de poser des questions en utilisant leurs propres termes, les aidant ainsi à naviguer de manière plus intuitive à travers le vaste assortiment de Zalando* »[15].

Néanmoins, l'utilisation de l'IA dans le secteur des paiements soulève également de nombreux défis telle que la confidentialité des données bancaires des utilisateurs. De la même manière, l'IA peut parfois donner lieu à des biais algorithmiques. Un tel risque doit être pris en compte car il pourrait impacter les décisions liées aux paiements et à la gestion des risques.

En somme, les avancées de l'IA dans les paiements sont particulièrement prometteuses. Celles-ci promettent de redéfinir l'écosystème financier, tout en nécessitant des garde-fous extrêmement rigoureux afin de se conformer à la réglementation et de garantir la sécurité des données.



Expérience utilisateur présentée par Zalando

[15] Press release - Zalando to launch a fashion assistant powered by ChatGPT, April 2023 (available here)

Conclusion – Se préparer pour 2030

L'industrie du paiement est à un moment charnière. Avec l'essor d'internet, elle a connu des transformations majeures ces deux dernières décennies avec une demande toujours plus forte pour des paiements digitaux comme illustrée par la montée en puissance du e-commerce et du m-commerce. On constate aujourd'hui une accélération de cette transformation grâce à de nombreuses technologies répondant aux attentes des utilisateurs pour des paiements toujours plus simples, sûrs, rapides et efficaces.

Pour les consommateurs et les commerçants, tout l'enjeu est de rendre le paiement à la fois omniprésent, car disponible dans chaque objet du quotidien, tout en étant invisible grâce à une expérience utilisateur sans couture. A cet égard, l'internet des objets et la biométrie, couplés à des technologies en plein développement comme la tokenisation s'annoncent révolutionnaires et devraient impacter de façon très positive le commerce.

Côté infrastructures, le défi consiste à répondre aux différents cas d'usage des utilisateurs en mettant en œuvre des rails de paiement à la fois distincts mais interopérables, garantissant un choix toujours plus important. A cet égard, la standardisation et la réutilisation d'infrastructures existantes apparaît comme un enjeu clé pour éviter une démultiplication de solutions de paiement qui risque de se faire au détriment de l'expérience utilisateur.

Enfin, la sécurité doit demeurer un impondérable pour les professionnels du paiement. Cette priorité doit nécessairement couvrir les menaces d'aujourd'hui tout en impulsant la migration nécessaire pour faire face aux attaques de demain. Le quantique illustre parfaitement la proactivité et l'agilité que les professionnels du paiement devront mettre en œuvre. Malgré cette course à l'innovation, la sécurité doit rester l'alpha et l'oméga de l'industrie pour maintenir la confiance des utilisateurs.

Dans ce paysage, la France a des atouts majeurs à faire valoir, avec notamment des décideurs ouverts à l'innovation et ayant fait le choix de réglementations en avance de phase pour apporter une certaine visibilité aux acteurs de marché. Cette visibilité est absolument clé pour que les acteurs du paiement puissent flécher les investissements massifs à réaliser dans la bonne direction. L'approche future-proof est incontournable pour éviter qu'un flou réglementaire ne s'installe, ce qui pénaliserait le commerce dans son ensemble.

Enfin, la France bénéficie d'un écosystème dynamique, comprenant un mélange d'acteurs financiers traditionnels, de Fintech innovantes et d'entreprises internationales présentes et actives sur le territoire ayant la masse critique pour porter des innovations de rupture. La coopération entre secteurs public et privé est notamment décisive pour trouver l'équilibre entre innovation et réglementation évoqué précédemment. A ce titre, la stratégie 2025-2030 du Comité national des moyens de paiement (CNMP) sera un document de référence pour cadrer les travaux collectifs. Cette approche en écosystème sur la base de l'expertise technologique des uns et des autres est une condition nécessaire pour que la France puisse être au rendez-vous de 2030, mais aussi de la décennie à venir.

the payments association