OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

La sécurité des paiements par crypto-actif

RAPPORT ANNUEL 2025 : EXTRAIT

BANQUE DE FRANCE
EUROSYSTÈME

www.observatoire-paiements.fr

OBSERVATOIRE DE LA SÉCURITÉ DES MOYENS DE PAIEMENT

La sécurité des paiements par crypto-actif

RAPPORT ANNUEL 2025 : EXTRAIT

Publication anticipée d'une étude du *Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2025* dont la parution est prévue au deuxième semestre 2026

AVRIL 2026

LA SÉCURITÉ DES PAIEMENTS PAR CRYPTO-ACTIF

1 Introduction

L'émergence de nouvelles technologies, comme les technologies des registres distribués [1] (DLT, *Distributed ledger technologies*), a permis le développement de nouveaux types d'actifs financiers. Parmi eux figurent les « crypto-actifs » qui peuvent être échangés entre acteurs économiques et servir de support pour régler des transactions [2] de détail et des transactions financières sans recourir, en principe, aux instruments de paiement scripturaux ou fiduciaires, ni aux infrastructures de marché traditionnelles. Ces actifs constituent ainsi la pierre angulaire de la « finance décentralisée » (DeFi, *decentralised finance*), qui vise à s'affranchir des canaux centralisés traditionnels de la finance et des paiements. Cette décentralisation signifie que le contrôle des transactions, les décisions et les validations sont opérés par un réseau de participants, selon des mécanismes définis par le réseau sous-jacent, sans autorité centrale unique.

Les crypto-actifs sont définis comme des représentations numériques d'une valeur ou d'un droit, pouvant être transférées et stockées de manière électronique, au moyen d'une DLT, comme la chaîne de blocs (*blockchain*), ou d'une technologie similaire. Leur émission et leur distribution sont régulées dans l'Union européenne par le règlement européen MiCA [3]. Pour la suite de cette étude, on entend deux types d'actifs :

- les crypto-actifs dits de « première génération », comme le Bitcoin ou l'Ether, qui ne sont adossés à aucune réserve d'actifs et connaissent une forte volatilité de leur valeur, liée à la rencontre de l'offre et de la demande, par rapport aux monnaies ayant cours légal ;
- les crypto-actifs dits de « deuxième génération », les « *stablecoins* », apparus pour tenter de remédier à cette volatilité, qui sont souvent adossés à un actif financier traditionnel (devise, matière première, titre, etc.) ou à un panier d'actifs (indice boursier, etc.). Lorsqu'ils sont conçus pour être utilisés comme actifs de règlement, ils sont en règle générale adossés à une monnaie ayant cours légal, avec une parité de 1:1. Au regard du règlement MiCA et des précisions apportées par l'Autorité bancaire européenne (ABE), ils sont alors qualifiés de « jetons de monnaie électronique » [4] (EMT, *e-money tokens*) et intègrent la qualification d'unités de monnaie électronique [5] en matière d'encadrement réglementaire (notamment la deuxième directive européenne sur les services de paiement – DSP2 – et la deuxième directive sur la monnaie électronique – DME2 [6]).

Du point de vue des infrastructures

Concernant leur fonctionnement, les transactions sur crypto-actifs sont enregistrées dans une chaîne de blocs [7], et sont distribuées par un réseau généralement public et décentralisé. Celui-ci a pour objectifs de regrouper, de sécuriser et d'horodater les transactions par le biais de moyens cryptographiques, afin de garantir leur traçabilité et leur intégrité. Ces technologies, prises individuellement, présentent parfois des similitudes à celles utilisées pour sécuriser des paiements classiques. Toutefois, leur association à la technologie de chaîne de blocs permet un fonctionnement entièrement décentralisé, sans tiers de confiance chargé d'assurer une tenue de compte de référence. En effet, chaque participant, ou « nœud », à la chaîne de blocs détient une copie du registre des transactions identique à celle des autres participants, rendant les tentatives de falsification plus complexes.

1 « Registre distribué » : répertoire d'informations qui conserve un enregistrement des transactions et qui est partagé et synchronisé au sein d'un ensemble de nœuds de réseau DLT, au moyen d'un mécanisme de consensus (article 3 du règlement européen MiCA, *Markets in Crypto-Asset Regulation*).

2 Les usages des crypto-actifs à des fins de règlement pour l'achat d'autres crypto-actifs (y compris les crypto-actifs uniques et non fongibles ou les actifs réels représentés sous la forme de jetons) sont exclus du périmètre de l'étude.

3 Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés des crypto-actifs.

4 EMT : « *e-money token* » émis par un établissement de monnaie électronique (EME) ou de crédit (EC).

5 Article L. 315-1 du Code monétaire et financier (CMF I. et II. : « La monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique […] et les unités de monnaie électronique sont dites unités de valeur ».

6 Directive européenne (UE) 2015/2366 relative aux services de paiement (DSP2), et directive 2009/110/CE sur la monnaie électronique (DME2).

7 Pour en savoir plus : « La *blockchain* », Banque de France, ABC de l'Économie, *L'Éco en Bref*.

Du point de vue des acteurs

En pratique, l'accès direct à la chaîne de blocs requiert des compétences et des moyens informatiques difficilement accessibles pour les utilisateurs traditionnels de paiement de détail, qu'il s'agisse de commerçants ou de particuliers. En conséquence, la mise en œuvre du paiement de détail par crypto-actif repose sur le recours à des intermédiaires spécialisés. Ces derniers délèguent ensuite l'exécution des échanges d'unités de crypto-actifs à travers la chaîne de blocs.

Tout au long du parcours de paiement par crypto-actif, divers acteurs interviennent en effet pour faciliter la réalisation du paiement, depuis l'utilisateur final jusqu'au commerçant acceptant ce mode de règlement. Ainsi, afin de relier les diverses parties prenantes aux paiements par crypto-actif, peuvent intervenir des acteurs comme les émetteurs de crypto-actifs, les plateformes d'échange [8] et les institutions bancaires, qui ont notamment la charge de reverser au commerçant le montant de la transaction en euros.

Des ponts avec le secteur des paiements « traditionnels » existent

Dans la quasi-totalité des cas, le commerçant préfère recevoir son paiement en monnaie ayant cours légal, c'est-à-dire en euros, ce qui nécessite une conversion préalable des crypto-actifs qui sont utilisés par le payeur avant que le produit de cette conversion ne soit reversé au commerçant.

Pour ce faire, différents parcours sont possibles, selon le type de paiement par crypto-actif : QR code [9], carte de paiement ou portefeuille de crypto-actifs. Cette conversion implique une association de services sur crypto-actifs et de services de paiement traditionnels.

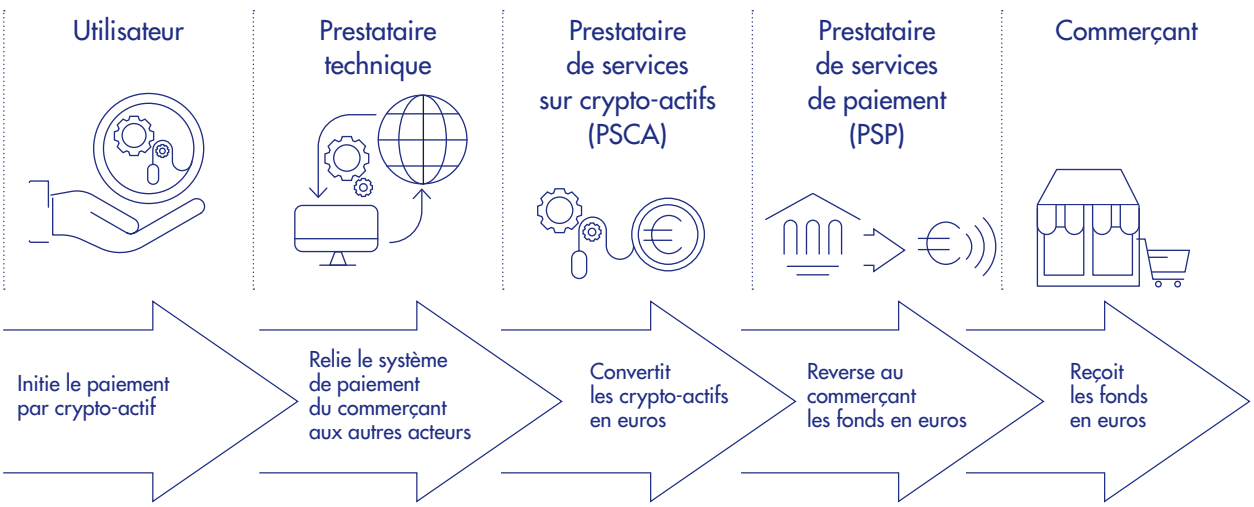
Les objectifs de cette étude

Dans le cadre du mandat de l'Observatoire, la présente étude se concentre sur l'analyse de la sécurité des paiements de détail par crypto-actif en France.

Les autres risques liés [10] à la détention ou à l'usage de crypto-actifs (risques de marché, de crédit, de liquidité ou encore de blanchiment de capitaux) ne sont donc pas évoqués dans le cadre de cette étude, mais doivent néanmoins être pris en considération par les acteurs qui souhaitent détenir ou échanger des crypto-actifs, ou plus largement, offrir des services sur crypto-actifs. De même, ce rapport ne se concentrera pas sur les aspects strictement juridiques des paiements par crypto-actif [11], ni sur les aspects fiscaux liés à de tels paiements.

Cette étude vise ainsi à dresser, pour la France, un panorama des solutions de paiement par crypto-actif à la suite de l'entrée en application du règlement européen MiCA, et à identifier les enjeux de sécurité propres aux paiements par crypto-actif. L'Observatoire émet, dans ce cadre, des recommandations en la matière.

S1 PANORAMA DES ACTEURS POUR UN PAIEMENT PAR CRYPTO-ACTIF



Source : Observatoire de la sécurité des moyens de paiement.

2 La typologie des paiements par crypto-actif

Les crypto-actifs de première génération (à l'instar du Bitcoin) peuvent être techniquement utilisés dans le cadre de paiements. Dans les faits toutefois, ils ne sont pas adaptés aux paiements du quotidien en raison de la volatilité de leur valeur, ainsi que des frais et délais associés à chaque transaction. C'est pourquoi l'analyse ci-après se concentre principalement sur les cas d'usage de paiement par *stablecoins*, tout en englobant, à la marge, certains cas d'usage de paiement par crypto-actif de première génération. En effet, dès lors que le commerçant préfère, en pratique, être réglé en euros, l'usage de *stablecoins* permet notamment une limitation du risque de change et de volatilité par rapport aux autres crypto-actifs lors de la conversion en monnaie ayant cours légal.

Il est à noter, de façon préliminaire, que **les crypto-actifs sont très peu utilisés dans les paiements de détail à ce jour sur le territoire français**. En effet, moins de 3 % [12] des Français indiquaient, en 2023, avoir déjà utilisé des crypto-actifs à des fins de paiement. *A fortiori*, le nombre de commerces de détail référencés acceptant directement le paiement par crypto-actif en France en 2025 est très faible. Par exemple pour le Bitcoin, il existe environ 300 accepteurs pour un total de 300 000 points de vente, ce qui représente seulement 0,1 % des points de vente totaux.

En outre, les crypto-actifs, dont les *stablecoins*, sont utilisés pour réaliser des opérations d'achat et de vente sur d'autres crypto-actifs, mais ils ne servent en pratique que très marginalement à l'achat de biens et de services traditionnels. En dehors des paiements de détail réalisés en France, on observe néanmoins le développement de l'utilisation des *stablecoins*, en particulier ceux régulés par MiCA. Ils sont essentiellement utilisés pour des transactions sur des marchés financiers, pour des paiements transfrontaliers entre professionnels et pour de la gestion de trésorerie, y compris à l'échelle de groupes.

2.1 Les paiements de proximité

D'un point de vue pratique, les paiements au point de vente par crypto-actif s'effectuent en s'appuyant sur des instruments similaires à ceux mis à disposition pour les paiements traditionnels. L'**initiation du paiement** passe ainsi, soit par le terminal de paiement électronique (TPE) du commerçant, qui génère un QR code comportant les informations relatives à la transaction, soit par la carte de paiement du client, qu'il s'agisse de la carte en elle-même ou qu'elle soit intégrée dans son mobile. Dans tous les cas, la solution d'**acceptation du paiement** par crypto-actif peut, quant à elle, être intégrée au système de caisse, ou alors être émise sur un support tel qu'une tablette ou un téléphone, utilisés comme solution d'encaissement mobile (*SoftPos*).

Dans le cas du paiement par QR code au point de vente, le client scanne, en premier lieu, le QR code généré par le TPE du commerçant. Selon les possibilités offertes par le commerçant, il choisit alors i) sa plateforme d'échange, ii) son portefeuille de crypto-actifs (s'il en dispose de plusieurs), puis iii) le crypto-actif avec lequel il souhaite payer. À l'étape suivante, le payeur valide l'opération auprès de la plateforme d'échange ou de l'émetteur d'EMT, qui la transmet ensuite au réseau de la chaîne de blocs. Enfin, la transaction est confirmée et la vente finalisée. S'ensuit une phase de conversion qui est neutre pour le payeur en matière de parcours client, pendant laquelle le paiement transite par une passerelle de paiement, chargée d'établir le lien entre les crypto-actifs et les canaux bancaires traditionnels (SEPA, etc.). La plateforme d'échange, ou l'émetteur d'EMT, convertit les crypto-actifs en monnaie ayant cours légal, et le montant en euros est ensuite reversé au commerçant par un prestataire de services de paiement.

Dans le cas du paiement par carte bancaire de proximité, le paiement passe par la mise en contact de la carte, aussi bien physique que virtuelle, avec un terminal de paiement. La carte est généralement préalimentée en crypto-actifs ou connectée à un portefeuille de crypto-actifs. Plusieurs options existent dans le choix du crypto-actif à utiliser pour le paiement. En principe, un choix par défaut est effectué par l'utilisateur pour les opérations à venir. Mais le choix peut basculer de façon automatique vers

8 Ces plateformes d'échange ont pour rôle de convertir les crypto-actifs présents sur le portefeuille de crypto-actifs (*wallet*) de l'utilisateur.

9 Le paiement par QR (*Quick Response*) code correspond à une solution de paiement numérique qui consiste, pour un payeur, à scanner un code bidimensionnel avec son téléphone afin d'initier la transaction.

10 « Crypto-actifs : l'AMF appuie l'appel à la prudence lancée par l'ESMA à destination des investisseurs individuels », AMF (18 décembre 2024). Pour rappel, les crypto-actifs sont très risqués car leur protection est faible de manière générale, et sont généralement moins encadrés que la plupart des autres types d'actifs, avec des acteurs parfois non régulés.

11 *Rapport sur l'évolution de la notion juridique de monnaie*, Haut Comité Juridique de Place (HCJP), juin 2025.

12 « Quel avenir pour le monde des crypto-actifs ? », Banque de France, 17 octobre 2024.

un autre actif lorsque le solde de crypto-actifs utilisés par défaut ne couvre pas la totalité du paiement. La conversion en monnaie ayant cours légal a ensuite lieu par le biais des passerelles de paiement sur une plateforme d'échange ou un autre prestaire de services sur crypto-actifs (PSCA), de façon identique au paiement par QR code. Enfin, la transaction s'effectue par l'intermédiaire des réseaux traditionnels de paiement par carte, jusqu'à réception des fonds par le commerçant, par l'intermédiaire de son prestataire de services de paiement (PSP).

Pour ces deux types de solutions de paiement par crypto-actif au point de vente, une connexion internet est le plus souvent nécessaire pour valider l'opération. Toutefois, selon le support [13] de paiement utilisé, il est parfois possible de payer hors-ligne, c'est-à-dire sans connexion internet directe, en utilisant la technologie NFC [14] ou par QR code.

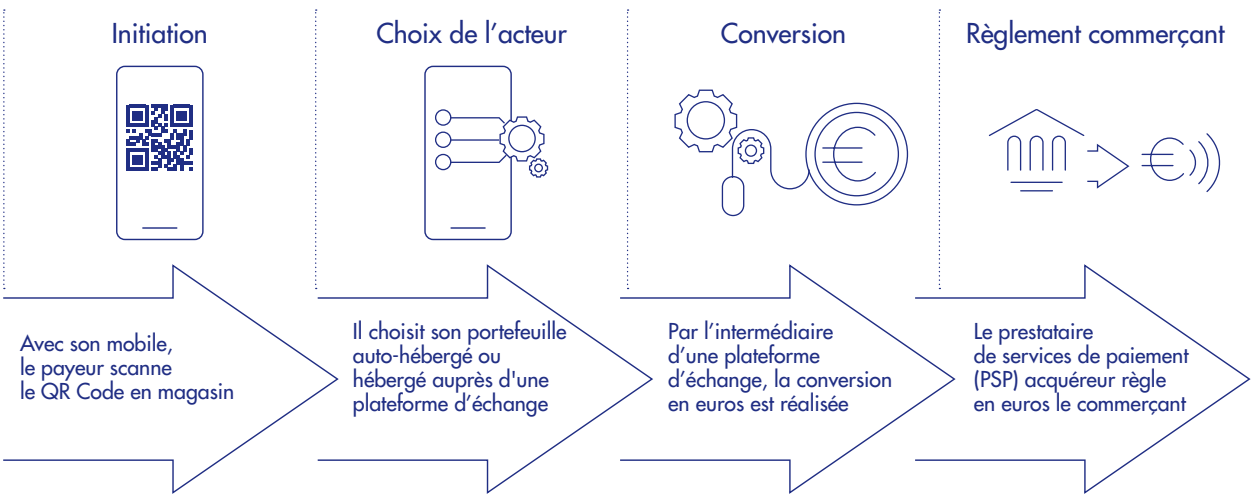
2.2 Les paiements à distance

Le paiement à distance par crypto-actif peut s'effectuer comme un paiement en *e-commerce* par un moyen de paiement classique (tel que la carte, le virement, ou à partir d'un compte de monnaie électronique), soit en se rendant sur le site du commerçant, soit à partir d'un lien de paiement généré par le commerçant. La possibilité de payer par crypto-actif apparaît alors au moment de choisir le moyen de paiement, au côté des autres moyens de paiement possibles. Ensuite, le paiement se déroule comme décrit précédemment, avec le choix de l'actif dans le portefeuille électronique, la réalisation de la transaction, puis la conversion pour régler le commerçant en monnaie ayant cours légal.

2.3 Les paiements de portefeuille à portefeuille

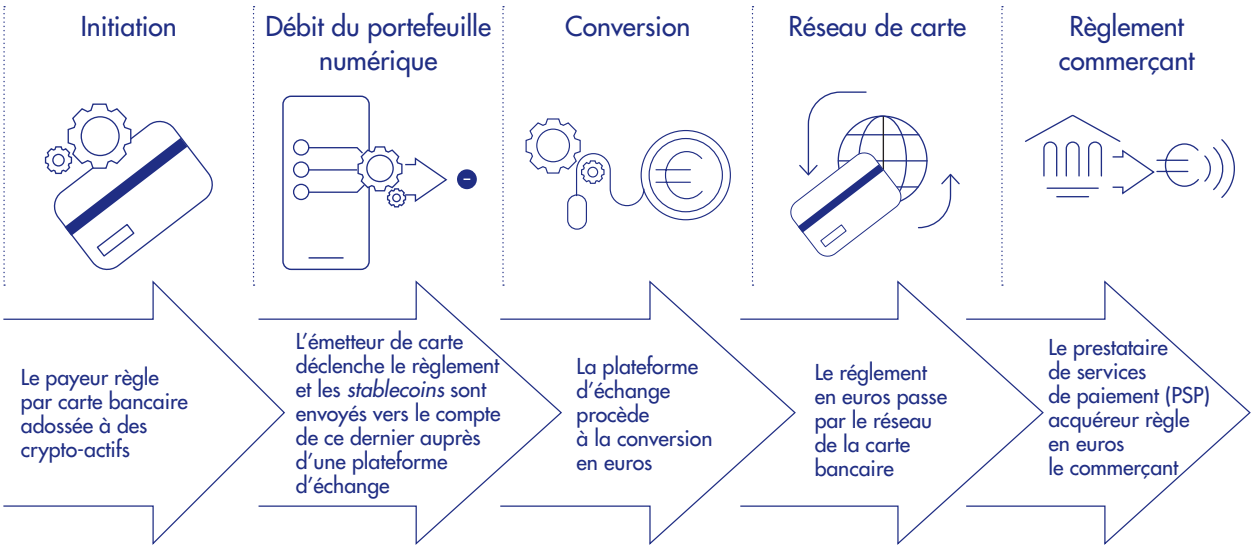
Une alternative existe, avec un usage très rare, lorsque l'utilisateur et le commerçant disposent tous les deux d'un portefeuille de crypto-actifs. Le paiement se fait alors par crypto-actif, directement d'un portefeuille à un autre, sans conversion en monnaie ayant cours légal. Ce cas de figure est quasi inexistant en France et concerne aussi bien les paiements à distance que ceux de proximité. Les risques sont accrus pour l'utilisateur dans le cas d'un paiement réalisé directement de portefeuille à portefeuille, lorsque les portefeuilles sont autohébergés (portefeuilles *non-custodial*) [15], ou d'un paiement par des crypto-actifs autres que des EMT.

S2 FLUX DE PAIEMENT DE PROXIMITÉ PAR QR CODE



Source : Observatoire de la sécurité des moyens de paiement.

S3 FLUX DE PAIEMENT DE PROXIMITÉ PAR CARTE BANCAIRE



Source : Observatoire de la sécurité des moyens de paiement.

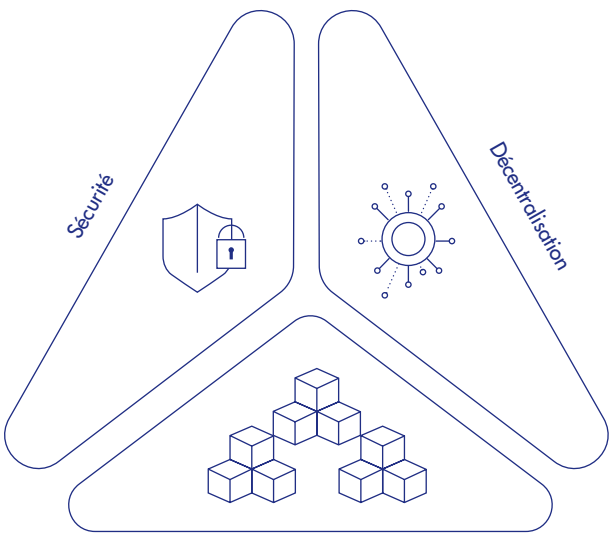
3 Le fonctionnement technique sous-jacent

Le principe de la chaîne de blocs réside en une infrastructure informatique implémentant des protocoles techniques, qui permettent le fonctionnement de l'ensemble du système.

Il existe deux grandes catégories de chaînes de blocs, déterminées par le mode de participation : permissionnée (souvent privée) et non permissionnée (souvent publique). Sur le plan technique, la méthode de fonctionnement est identique pour les deux catégories. Ce qui les distingue sont leurs accès. En matière de chaîne de blocs privée, les opérations ne sont visibles que par les participants ayant la permission d'y accéder. L'accès est donc limité et par conséquent la transparence partielle. *A contrario*, lorsque la chaîne de blocs est publique, les opérations sont visibles par tous et réputées immuables, avec des frais de réseau parfois élevés.

En phase de conception d'une chaîne de blocs, les principaux objectifs recherchés sont i) la sécurité du réseau, ii) sa décentralisation (contrôle effectué par plusieurs acteurs) et iii) sa scalabilité (capacité à faire un grand nombre de transactions, plus rapidement et à moindres frais). Ces objectifs sont difficilement conciliables, ce qui constitue une forme de trilemme. Le fonctionnement des chaînes de blocs a donc évolué au cours des dernières années pour trouver un équilibre optimal, en fonction des usages et des attentes du marché.

S4 TRILEMME DE LA CHAÎNE DE BLOCS



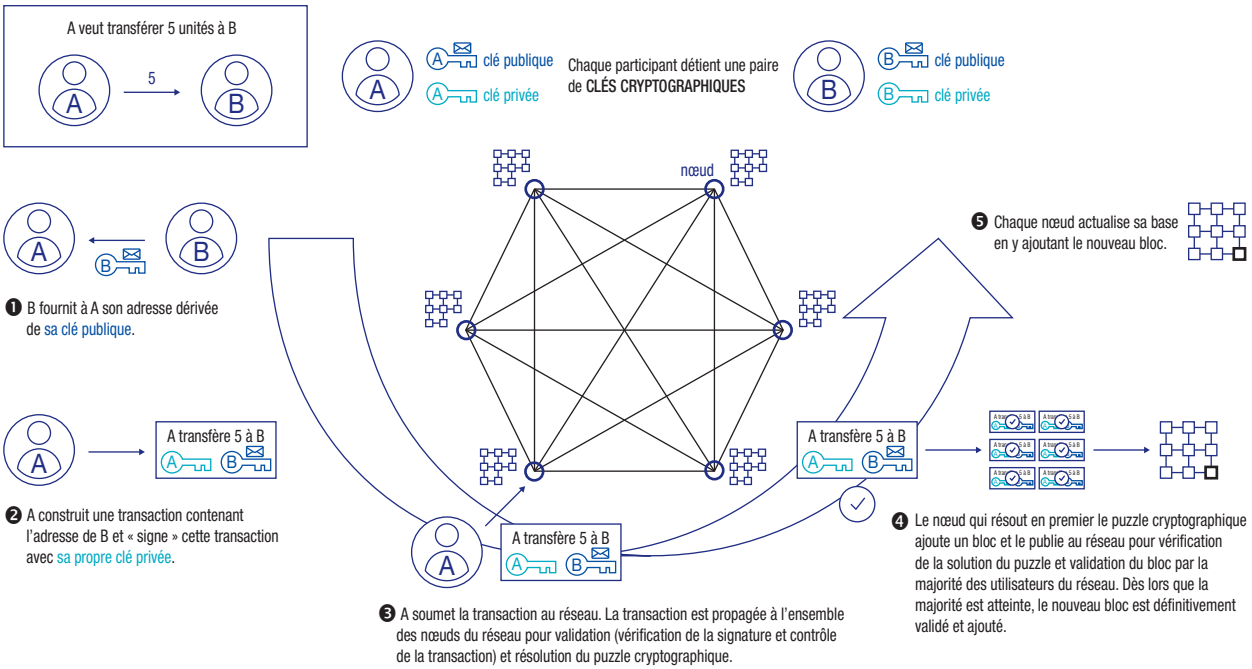
Source : Observatoire de la sécurité des moyens de paiement.

13 Portefeuille « *self-custody* », portefeuille matériel (*hardwallet*) ou cartes de paiement spécifiques.

14 « *Near Field Communication* » : technologie permettant un partage de données à très courte portée entre des appareils compatibles.

15 Dans ce cas, les clés privées sont stockées localement sur l'appareil.

S5 VALIDATION D'UNE TRANSACTION DANS UNE CHAÎNE DE BLOCS À PREUVE DE TRAVAIL



Source : Banque de France (ABC de l'Économie, *L'Éco en Bref*, « La *blockchain* »).

3.1 Les chaînes de blocs natives

À l'origine, la chaîne de blocs repose sur une première couche, dite « couche 1 », qui permet d'enregistrer des transactions directement sur la chaîne (*on-chain*). Elle garantit la sécurité et la décentralisation du processus par des mécanismes de consensus [16]. Ces derniers consistent, pour un réseau de nœuds [17], à valider les transactions, sans l'intervention d'une autorité centrale, en utilisant différents protocoles [18]. Cette chaîne de blocs dite « d'infrastructure » a des fonctionnalités de sécurité, gouvernance, consensus et exécution.

La structure de ce sous-jacent technologique se décompose principalement en trois volets :

- **le réseau**, qui s'apparente à plusieurs ordinateurs ou serveurs – nœuds –, qui exécutent un algorithme afin de sécuriser le système en recevant les transactions, les validant selon les règles du protocole utilisé et stockant les blocs ;
- **les blocs**, qui comprennent un ensemble de transactions, dont le nombre peut varier selon la chaîne utilisée ;
- et **une chaîne**, qui relie les blocs de bout en bout en utilisant des moyens cryptographiques [19], à travers un hachage. Ce hachage consiste en une empreinte digitale non modifiable, permettant de sécuriser la transaction. En pratique, les données contenues dans le bloc précédent sont chiffrées, et ainsi figées.

Le délai d'exécution peut s'avérer long et coûteux en fonction de plusieurs facteurs :

- le nombre d'ordinateurs en charge de valider l'opération. Selon le réseau et le nombre de validateurs actifs, le traitement des transactions peut être plus ou moins rapide ;
- les frais. Les transactions avec des frais de réseau plus importants sont priorisées par les « nœuds », car c'est par ce biais que les validateurs de ces nœuds sont rémunérés. Ces frais sont plus communément appelés « frais de gaz » (« *gas fee* », soit les frais de réseau).

- la congestion du réseau. Le nombre de nœuds [20] actifs étant fixe, si les transactions s'accumulent, elles peuvent être mises en attente avant de disposer d'un nouveau bloc qui pourra les contenir.

⇨ Pour des opérations de faible montant, les frais de réseau ne sont pas négligeables et la transaction peut mettre une dizaine de minutes à être validée, voire parfois davantage, avec un risque de congestion du réseau. Pour ces raisons, les paiements par crypto-actif reposant sur la couche 1 ne semblent pas adaptés à la réalisation d'achats de biens ou de services au quotidien, et ne sont donc pas – ou très rarement – utilisés comme tels. Cette complexité technique explique notamment l'utilisation marginale, voire quasi inexistante, des crypto-actifs au sens strict parmi les solutions de paiement proposées par les professionnels en France. Ces actifs sont ainsi presque exclusivement utilisés comme actifs spéculatifs à des fins d'investissement.

3.2 Les chaînes de blocs spécifiques

L'introduction d'une couche supplémentaire de blocs, dite « couche 2 », vise à accélérer et à améliorer les performances de l'ensemble de la chaîne de blocs. Pour ce faire, les transactions sont traitées en dehors de la chaîne de blocs principale (*off-chain*), puis validées dans la couche 1. Les transactions sont ainsi agrégées et traitées en masse, ce qui permet de gérer un plus grand nombre de transactions et de réduire les coûts associés.

Cette couche 2 est en constante évolution au gré de l'innovation et plusieurs modèles existent à l'heure actuelle. Par exemple, le protocole « *rollup* optimiste » part du postulat que les transactions sont valides en l'absence de preuve de fraude par les mécanismes de détection. Le séquenceur, composant opérationnel du *rollup*, va collecter, ordonner et exécuter plusieurs opérations en dehors de la chaîne de blocs. Il traite donc plus rapidement les transactions, et réduit ainsi les frais. Les transactions sont, par ce moyen, regroupées en lot [21]. Dans ce cas, un résumé de l'ensemble des transactions est publié sur la couche 1 et les transactions ne sont pas vérifiées immédiatement sur cette couche 1. Une vérification détaillée peut avoir lieu, *a posteriori*, pendant la période de contestation en cas de fraude. Sur la chaîne de blocs de couche 2, des « contrats intelligents » (*smart contracts* [22]) applicatifs vont permettre de traiter toutes les étapes et, sur la chaîne de base en couche 1, des contrats intelligents de contrôle vont ensuite permettre d'assurer la sécurité. Une autre méthode, utilisée par le « *ZK rollup* [23] » (*zero-knowledge rollup*), consiste à sécuriser davantage les opérations en générant des preuves cryptographiques pour les garantir. Ces preuves sont ainsi enregistrées sur la couche 1 sans révéler les détails des transactions.

Très récemment, une « couche 3 » a également émergé. Il s'agit d'une couche applicative améliorant l'interopérabilité entre couches. La couche 3 vise ainsi à connecter les couches 1 et 2 de la chaîne de blocs avec les applications et services inhérents, sans l'intervention d'un tiers.

Ces couches supplémentaires qui viennent s'ajouter à la chaîne de blocs d'origine jouent un rôle essentiel dans le développement de ces nouvelles technologies. Elles garantissent la possibilité d'accroissement de l'écosystème et l'interaction de ses composantes.

⇨ L'interopérabilité constitue en effet un enjeu intrinsèque des aspects technologiques. Chaque réseau de chaîne de blocs dispose de ses propres standards, ce qui rend ainsi nécessaire l'utilisation de passerelles et génère donc un premier point de vulnérabilité potentiel sur la chaîne de paiement.

16 Processus défini en amont, par lequel la transaction s'effectue.

17 Réseau composé de machines/ordinateurs qui contribuent au stockage, à la validation/vérification et à l'échange d'informations sur les transactions.

18 Preuve de travail (*proof of work*) ou preuve d'enjeu (*proof of stake*).

19 La sécurité cryptographique est intégrée dans le protocole de la chaîne de blocs, de sorte que l'utilisateur final dispose d'une clé privée pour signer la transaction. La vérification de la signature s'effectue de façon décentralisée, avec une clé publique.

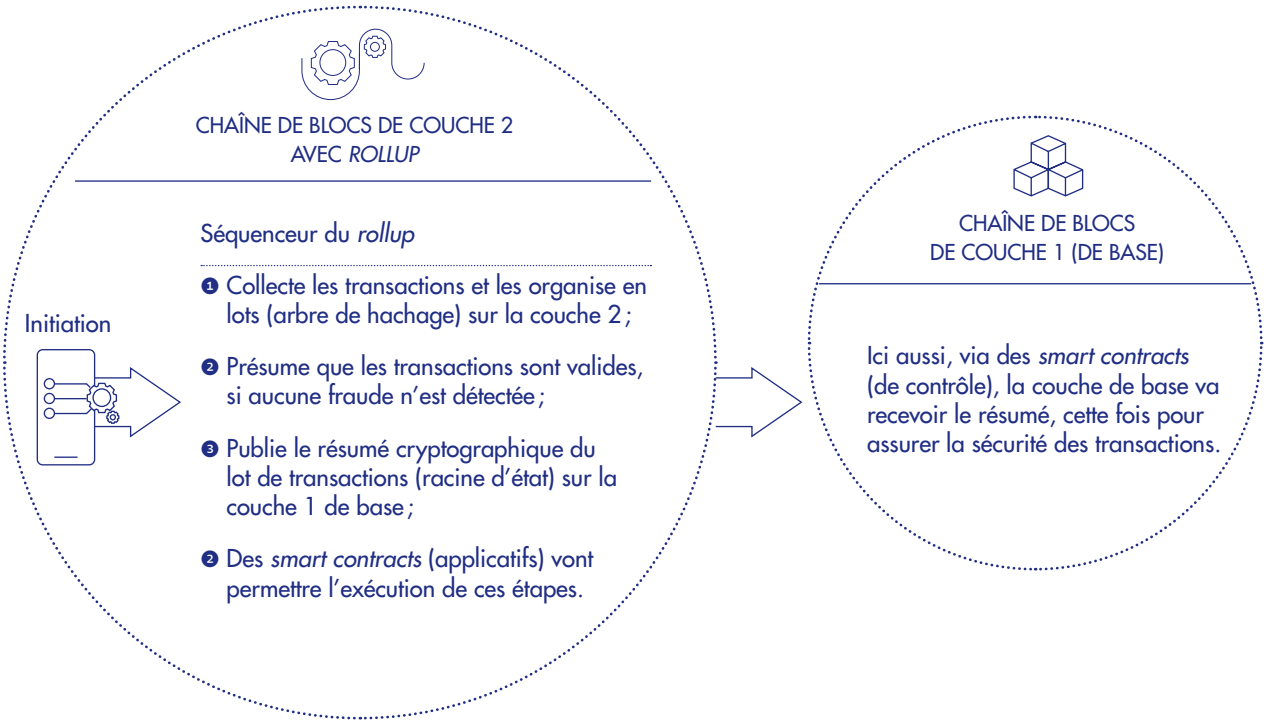
20 Par exemple, le nombre de nœuds pour les principaux réseaux : jusqu'à 2 500 pour Bitcoin, 1 400 pour Ethereum, 5 000 pour Solana ou 2 000 pour Polygon.

21 Elles sont regroupées et organisées selon un « arbre de hachage » (ou arbre de *Merkle*). Il s'agit d'une structure de données utilisée en cryptographie pour réduire les quantités de données qui doivent être conservées dans une chaîne de blocs à des fins de vérification. Le hachage de la racine résume toutes les données contenues individuellement dans chaque transaction traitée au sein du même lot.

22 Programme autonome déployé sur une chaîne de blocs, qui exécute automatiquement des règles prédéfinies.

23 Rapport sur la finance décentralisée, *Decentralised Finance (DeFi)*, *European Union Blockchain Observatory and forum* (Observatoire et Forum de la blockchain de l'Union européenne), 24 mai 2022 : *« Un* Zero-Knowledge (ZK) rollup *est une solution de mise à l'échelle qui exécute les transactions hors chaîne, puis publie sur la couche 1 une preuve cryptographique de validité (*Zero-Knowledge Proof*). Cette preuve garantit la conformité des transactions sans divulguer leurs données, ce qui réduit la quantité d'informations à publier sur la* blockchain *principale »*.

S6 ILLUSTRATION DU « *ROLLUP* », PROTOCOLE D'UNE CHAÎNE DE BLOCS DE COUCHE 2



Source : Observatoire de la sécurité des moyens de paiement.

4 Les enjeux de sécurité

Les risques auxquels sont exposés les paiements par crypto-actif sont de deux ordres : i) les risques « classiques », affectant l'utilisation des moyens de paiement traditionnels, et ii) les risques plus spécifiquement attachés à l'utilisation des crypto-actifs, qui ont trait aux caractéristiques techniques inhérentes à ces nouveaux actifs de règlement.

4.1 Les risques dits « classiques »

Bien qu'il ne s'agisse pas d'une caractéristique propre aux paiements par crypto-actif, il est essentiel de souligner, à titre liminaire, que les arnaques et fraudes en ligne qui utilisent les crypto-actifs comme supports se sont accrues. Elles doivent donc constituer un point d'attention majeur pour les utilisateurs potentiels.

De façon générale, lorsque le paiement par crypto-actif est réalisé avec une carte de paiement classique, l'utilisateur est exposé aux risques attachés à une transaction par carte. En matière de sécurité, les normes ISO [24] avec des champs cryptographiquement protégés sont souvent utilisées. De plus, les données de paiement sont chiffrées par l'utilisation d'algorithmes de chiffrement symétrique (AES – *Advanced Encryption Standard*) et asymétrique (RSA – du nom des initiales de ses trois inventeurs). Parallèlement, la chaîne de traitement du paiement est certifiée par la norme de sécurité des données de l'industrie des cartes de paiement PCI-DSS (*Payment Card Industry – Data Security Standard*). Cependant, les chiffrements actuels ne sont pas tous post-quantiques et peuvent ainsi présenter une vulnérabilité face aux attaques.

⇨ Mettre en place des démarches d'adaptation au chiffrement post-quantique s'avère donc nécessaire, conformément aux recommandations [25] déjà édictées par l'Observatoire afin de prévenir ce risque de résilience opérationnelle.

De même, l'utilisation du QR code peut également constituer une faille, notamment car les fraudeurs peuvent le falsifier (*quishing*). Dans ce cas, le fraudeur remplace le QR code du commerçant par le sien afin de recevoir les paiements à la place du commerçant. Ce procédé

a déjà été observé dans le cadre de l'utilisation de ce mécanisme d'initiation de paiement. En effet, certains commerçants mettent à disposition de leur clientèle un QR code statique, qui constitue un facteur de risque, car ce type de QR code n'est pas limité dans le temps et peut donc être plus facilement falsifiable.

⇨ Le QR code dynamique, quant à lui, possède une durée limitée et permet ainsi de réduire le risque de fraude associé à ce mécanisme.

De manière générale, la multiplicité des acteurs intervenant dans le processus de paiement par crypto-actif, tel que décrit précédemment, affecte la fluidité de l'acte de paiement (et prolonge donc sa durée). De surcroît, cette multitude d'intervenants compromet la résilience de la chaîne des paiements, en introduisant autant de points de vulnérabilité potentiels.

En outre, ces solutions de paiement présentent une résilience moindre que les paiements scripturaux classiques. Par exemple, une panne récente chez un important fournisseur *cloud* [26] a provoqué des interruptions dans les services de plusieurs acteurs de la sphère des crypto-actifs. Ce dysfonctionnement a concerné l'accès aux réseaux de chaînes de blocs, aux interfaces de programmation d'application (API – *Application Programming Interface*) de paiement et aux portefeuilles électroniques des utilisateurs. La capacité de résilience repose également sur les choix d'hébergement. La concentration vers un nombre limité de fournisseurs de services critiques – c'est-à-dire qui peuvent influer sur la sécurité et la performance du dispositif – peut effectivement soulever des difficultés lorsque la réplication des données est effectuée auprès de deux sites appartenant à un même fournisseur *cloud*.

⇨ Le renforcement du Plan d'Urgence et de Poursuite des Activités (PUPA) est donc une nécessité face aux éventuels risques de résilience opérationnelle, qui sont largement accrus par l'utilisation de crypto-actifs comme moyens de paiement et par la multiplicité des acteurs qui interviennent lors de ces parcours de paiement.

4.2 À ces risques dits « classiques », s'ajoutent de nouveaux risques spécifiques à l'utilisation des crypto-actifs

4.2.1 Le risque de sécurité des chaînes de blocs

Les chaînes de blocs reposent sur des principes de cryptographie, de décentralisation et de consensus, qui visent à assurer leur sécurité de manière intrinsèque. Ces principes natifs ne sont pour autant pas infaillibles, à plus forte raison dans le contexte actuel d'accumulation des couches, qui a pour objectif d'optimiser le fonctionnement des chaînes de blocs.

La sécurité des chaînes de blocs dépend donc fortement de la robustesse des infrastructures techniques et des protocoles sous-jacents. La fiabilité des nœuds, la résilience des fournisseurs *cloud*, la sécurité des API et la sécurité des « contrats intelligents » sont autant de facteurs critiques à prendre en compte.

⇨ Dans ce contexte, une évaluation rigoureuse de la solidité opérationnelle des composants techniques est indispensable pour garantir la sécurité des paiements par crypto-actif.

4.2.2 Le risque de perte/vol de clés privées et de fuites de données

Il existe différentes sortes de portefeuilles de crypto-actifs. Les deux principaux sont le portefeuille physique (*hard wallet*) et le portefeuille numérique (*hot wallet* ou *software wallet*). Le premier dispose de clés privées stockées sur un support, comme une clé USB ou une puce sécurisée. Le second possède des clés privées stockées sur un appareil connecté à internet, lorsqu'il s'agit d'un portefeuille autohébergé, ou en ligne sur un serveur distant, pour tout portefeuille hébergé (portefeuille *custodial*) [27]. Des clés asymétriques sont ainsi utilisées pour sécuriser les portefeuilles numériques avec, d'une part, la clé privée pour signer la transaction et, d'autre part, la clé publique pour recevoir les fonds. Par conséquent, pour un achat, l'utilisateur final de la chaîne de blocs va disposer d'une clé privée pour signer la transaction sur son portefeuille numérique, tandis que la clé publique – assimilable à l'identité bancaire d'un compte classique – consiste en l'adresse de réception des fonds. Cette clé publique peut, par exemple, être communiquée par le biais du QR code présenté par le commerçant au client.

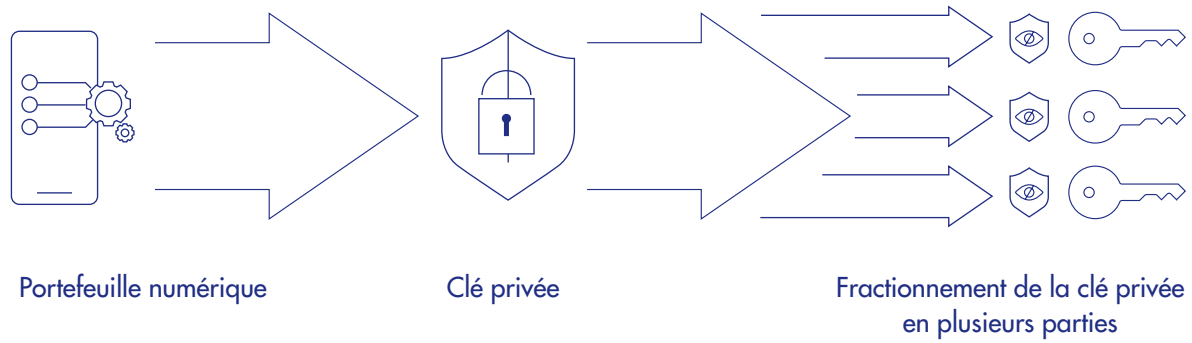
24 Normes définies par l'Organisation internationale de normalisation (ISO) et s'appliquant aux produits et aux services.

25 Chapitre 3 (pages 73-90) du *Rapport annuel de l'OSMP 2023* : « L'informatique quantique et la sécurité des systèmes de paiement par carte bancaire ».

26 Prestataire de services informatiques (hébergement d'infrastructure, de données, etc.).

27 Les clés privées sont conservées sur les serveurs d'un tiers comme une plateforme d'échange.

S7 PORTEFEUILLE QUI UTILISE LA MÉTHODE DE CALCUL MULTIPARTITE SÉCURISÉ (MPC – MULTI-PARTY COMPUTATION)



Source : Observatoire de la sécurité des moyens de paiement.

⇨ Les clés privées, qu'elles soient stockées sur un portefeuille physique ou numérique, constituent des données sensibles de paiement à protéger. Elles doivent donc être sécurisées afin d'éviter la perte irréversible d'accès aux crypto-actifs ou une compromission susceptible de permettre à un tiers malveillant de réaliser des opérations non autorisées. Cette sécurisation consiste notamment en des mises à jour régulières des appareils et moyens de stockage des clés privées vers les versions actualisées, ainsi qu'en la protection contre les connexions non sécurisées, comme les réseaux publics non sécurisés, en utilisant par exemple un réseau privé virtuel (VPN – *Virtual Private Network*).

Par ailleurs, les techniques de fraude pour obtenir les clés privées, qui donnent accès au portefeuille de crypto-actifs et permettent donc de réaliser des paiements, sont semblables à celles utilisées pour les paiements traditionnels : *phishing*, *smishing*, faux sites, etc.

⇨ Des versions plus sécurisées existent cependant, comme les portefeuilles intégrant soit des protocoles multisignatures soit la méthode de calcul multipartite sécurisé (MPC – *multi-party computation*). Plus adapté aux paiements de détail, le portefeuille utilisant la méthode MPC est une solution cryptographique dans laquelle la clé privée n'est pas présente sous sa forme complète en un seul endroit. Elle est fragmentée par des protocoles de calcul multipartite entre le payeur, le fournisseur de services et, potentiellement, un tiers de confiance. Par conséquent, la compromission de la clé privée devient plus difficile.

4.2.3 Les risques afférents aux « contrats intelligents » (*smart contracts*)

Un autre point de vulnérabilité potentiel réside dans le fait que les paiements par crypto-actif s'effectuent le plus souvent via des automates exécuteurs de clauses prédéfinies au niveau des chaînes de blocs, dits « contrats intelligents ». Concrètement, il s'agit de codes informatiques dans un langage de programmation spécifique à la chaîne de blocs utilisée. L'objectif est de définir, en amont, les conditions d'exécution des opérations, qu'il s'agisse d'émission d'unités de crypto-actifs ou de transactions, et d'encadrer les rôles et fonctions des parties prenantes. Par exemple, ces contrats intelligents permettent de conditionner l'exécution d'un paiement à la réalisation d'une condition externe, comme l'approvisionnement du compte ou l'autorisation d'un transfert, et de planifier des transactions récurrentes à exécuter. Or, le « contrat intelligent » peut être modifié lors d'une attaque externe qui utilise les méthodes classiques des attaques informatiques, par exemple, ou d'une fraude interne. Celle-ci est réalisable par une personne ayant une capacité d'action au sein d'une entité exploitant le contrat intelligent. Une fois ce contrat modifié, le fraudeur peut alors commettre une grande variété de fraudes : obtenir un accès à des portefeuilles d'actifs, réaliser des paiements frauduleux, etc.

L'OWASP – *Open Web Application Security Project* –, organisation internationale à but non lucratif dédiée à la sécurité des applications web, a ainsi procédé à une identification des dix plus importantes vulnérabilités des « contrats intelligents », dont elle tire plusieurs recommandations en matière de sécurité [28].

Illustration des principales vulnérabilités des « contrats intelligents »

1. L'attaque de « réentrance » : elle peut donner lieu à un détournement de fonds par un fraudeur, qui réussit à exécuter plusieurs fois une fonction du programme avant la mise à jour du « contrat intelligent », pour que l'opération apparaisse comme effectuée (cas du piratage « PenPie Hack » en 2024).
2. Défaillance du contrôle d'accès : le fraudeur réussit à entrer dans des fonctions du programme qui ne devraient être accessibles qu'à l'administrateur, comme les remboursements, afin de détourner des fonds (attaque de Bybit en février 2025).
3. Faille de la vérification de dépassement lors du calcul de liquidité : faille dans le contrat intelligent qui permet au pirate informatique de tromper le programme en lui faisant croire qu'il ajoute plus de liquidités qu'en réalité. À cause de cette manipulation, le contrat calcule des prix faussés, ce qui autorise l'attaquant à retirer plus d'actifs qu'il n'en a réellement apporté (attaque contre Cetus en mai 2025).

La sécurité des « contrats intelligents » est donc un enjeu essentiel. Les acteurs ont ainsi mis en place de bonnes pratiques, comme l'audit de ces « contrats intelligents » par un tiers indépendant. Certains auditeurs indépendants sont qualifiés « prestataires d'audit de la sécurité des systèmes d'information » (Passi) par l'Agence nationale de la sécurité des systèmes d'information (Anssi) [29], ce qui garantit leur expertise en matière de cybersécurité.

⇨ Par ailleurs, l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) ont publié le *Rapport d'un groupe de travail sur la certification des « contrats intelligents »*. Des pistes de réflexion y sont mises en lumière pour orienter i) la définition de standards de certification des « contrats *intelligents* », avec les grands principes de sécurité que ces derniers pourraient comprendre, ii) l'utilisation des méthodes d'audit existantes dans le cadre de cette certification, les organismes et moyens susceptibles de les mettre en œuvre, et iii) des pistes réglementaires qui pourraient intégrer un éventuel schéma de certification.

4.2.4 La surveillance en temps réel des couches 1 et 2

Outre les risques attachés à la chaîne de blocs primaire (couche 1), les traitements réalisés au sein de la couche 2 doivent également être surveillés, en tant que circuits externes à la chaîne de blocs primaire dont le résultat est ensuite déversé dans celle-ci. Le pont entre la couche 1 et la couche 2 peut également présenter un point de vulnérabilité.

⇨ Il est donc nécessaire d'exercer une surveillance en temps réel des paiements par crypto-actif, au même titre que les paiements traditionnels. L'objectif est de lutter efficacement contre la fraude en assurant une sécurité opérationnelle pour contrer les attaques et détecter les opérations frauduleuses.

5 Les enjeux de conformité

5.1 Les enjeux liés à la sécurité du parcours de paiement

Les solutions de paiement par crypto-actif doivent répondre à des obligations réglementaires en matière de sécurité du parcours de paiement, sur lesquelles s'appuie cette étude, tout autre aspect réglementaire en étant exclu. L'application des règles issues de la deuxième directive européenne sur les services de paiement (DSP2) est ainsi obligatoire pour les crypto-actifs, qualifiés de « jetons de monnaie électronique » (EMT) et donc assimilés à des fonds. En revanche, leur application n'est pas strictement obligatoire pour les solutions de paiement reposant sur des crypto-actifs qui ne sont pas qualifiés de fonds. Il s'agit notamment des crypto-actifs de première génération ou des « jetons se référant à un ou plusieurs actifs » (ART – *asset-referenced tokens*). En conséquence, certains acteurs non régulés proposent des solutions de paiement par des crypto-actifs autres que les EMT régulés, qui présentent donc un risque non négligeable pour les utilisateurs.

⇨ En s'appuyant sur le principe « *même activité, mêmes risques* », il est recommandé que ces règles soient observées par tous les acteurs, régulés ou non, pour leurs solutions de paiement reposant sur des crypto-actifs, quelle que soit la qualification juridique du crypto-actif. Cela concerne notamment les exigences en matière d'authentification forte des transactions.

28 Sur le site OWASP Smart Contract Security.

29 Référentiels d'exigences pour la qualification – Référentiel Passi.

Les règles de sécurité issues de la DSP2 s'appliquent aux crypto-actifs qualifiés de jetons de monnaie électronique, en particulier celles sur l'authentification forte [30] pour les paiements en ligne, le code confidentiel pour les opérations par carte supérieures à 50 euros ou encore la biométrie pour les transactions mobiles. Au-delà du paiement, les PSCA doivent également s'assurer de l'authentification forte de l'utilisateur final. Celle-ci permet de sécuriser l'accès au portefeuille de crypto-actifs ou la réalisation d'opérations sensibles (modification de mot de passe ou d'IBAN, enregistrement d'un nouvel appareil de confiance, etc.).

⇨ À cet égard, la révision en cours menée sur le paquet législatif DSP3/PSR et ses éventuelles implications réglementaires pour les acteurs concernés sur la chaîne des paiements par crypto-actif devront être suivies attentivement. En effet, il convient de garantir la bonne conformité de l'ensemble des acteurs du secteur aux exigences de sécurité mises en place par les cadres coordonnés DSP et MiCA, à travers l'articulation des statuts de PSP et PSCA notamment.

À ce titre, sur demande de la Commission européenne, l'ABE a publié, en juin 2025, un avis soulignant, en particulier, la nécessité du respect de certaines dispositions de la DSP2. Parmi elles se trouvent l'authentification forte du payeur pour l'accès aux portefeuilles de crypto-actifs ou encore le signalement des fraudes aux paiements. L'objectif est d'assurer, par ce moyen, un niveau de protection des consommateurs élevé, quels que soient les moyens de paiement utilisés (jetons de monnaie électronique ou fonds « traditionnels »). L'ABE rappelle également que les consommateurs et les autres acteurs du marché doivent être protégés de manière adéquate et avoir un degré élevé de confiance dans la stabilité du marché et la fiabilité des opérations de paiement, afin de permettre des paiements de détail efficaces et sûrs.

5.2 Les enjeux liés à la sécurité du système de paiement

Le règlement européen DORA (*Digital Operational Resilience Act*) relatif à la cyber-résilience du secteur financier impose aux PSCA les mêmes obligations qu'aux PSP en matière de cybersécurité, ainsi que la mise en place de tests et procédures pour encadrer et protéger les systèmes d'information. Néanmoins, à ce stade, l'infrastructure de chaîne de blocs n'étant pas réglementée, l'utilisation d'une nouvelle chaîne de blocs par l'émetteur de crypto-actifs n'est pas encadrée et peut donc susciter des problématiques de sécurité. Toute nouvelle utilisation doit ainsi être portée à la connaissance des autorités et des détenteurs de crypto-actifs dans le cadre du livre blanc (*whitepaper*) rédigé par l'émetteur et requis par le règlement MiCA.

⇨ En ce sens, l'analyse des risques, intégrant notamment un audit, en amont, et un audit régulier des chaînes de blocs, en aval, compte tenu des éventuelles nouvelles fonctionnalités ajoutées, sont de bonnes pratiques supplémentaires à encourager pour sécuriser dans le temps une infrastructure de chaîne de blocs.

Ces enjeux de résilience concernent également les infrastructures existantes. Les PSCA doivent donc se conformer aux exigences des règlements MiCA et DORA et, notamment, mettre en place des politiques de gestion opérationnelle des risques informatiques.

5.3 Les enjeux liés à la sécurité des acteurs et des actifs du paiement

Au-delà des aspects de sécurité, l'acceptation des paiements par crypto-actif implique pour les professionnels – commerçants ou prestataires techniques intégrant la solution de paiement – de recourir à un prestataire tiers dûment agréé.

⇨ L'acteur en charge de l'exécution de la transaction et de la conversion des crypto-actifs en monnaie ayant cours légal doit nécessairement être agréé en tant que PSCA (auprès de l'AMF s'il est établi en France) [31]. L'acteur qui procède au versement en euros sur les comptes du commerçant doit être agréé comme PSP ou autorisé en tant qu'agent de PSP (auprès de l'ACPR s'il est établi en France).

De la même manière, les crypto-actifs proposés par les acteurs doivent être conformes aux exigences réglementaires. À cet égard, les commerçants et leurs prestataires doivent sélectionner les actifs avant de les accepter pour paiement et strictement refuser ceux non conformes à la réglementation.

⇨ À ce titre, plusieurs autorités de marché, dont l'AMF [32], appellent à un cadre européen renforcé des marchés de crypto-actifs (ajustement potentiel du règlement MiCA). Elles sollicitent la prise en compte d'enjeux, en particulier, de renforcement des règles pour les plateformes opérant hors de l'Union européenne, un meilleur encadrement des plateformes face au

risque cyber, et une supervision directe par l'Autorité européenne des marchés financiers (AEMF) pour les PSCA significatifs. L'objectif est d'assurer une application uniforme des règles pour les acteurs européens.

30 Les règles européennes sur l'authentification forte sont notamment précisées dans un acte délégué de la DSP2 : le règlement (UE) n° 2018/389 détaillant les transactions assujetties.

31 L'émission de jetons de monnaie électronique est réservée aux établissements de crédit (EC) et aux établissements de monnaie électronique (EME). La fourniture de services sur crypto-actifs, dont la liste est définie à l'article 3 du règlement MiCA, est réservée aux prestataires de services sur crypto-actifs (PSCA).

32 AMF, 15 septembre 2025 : « Les autorités de marché française, autrichienne et italienne appellent à un cadre européen renforcé des marchés de crypto-actifs ».

RECOMMANDATIONS

L'Observatoire rappelle, en premier lieu, que les crypto-actifs présentent de nombreux risques (volatilité, liquidité, défaillance, blanchiment des capitaux et financement du terrorisme, frais transactionnels élevés, etc.), qui ne relèvent pas des strictes problématiques de sécurité adressées au travers des recommandations ci-après. Ils nécessitent une vigilance renforcée de la part de leurs utilisateurs et des autorités compétentes.

À la suite de cette étude de veille, l'OSMP émet les recommandations suivantes concernant la sécurité des solutions de paiement par crypto-actif dans le cadre de l'achat de biens et services au quotidien :

RECOMMANDATIONS À L'ATTENTION DES CONSOMMATEURS ET COMMERÇANTS

Recommandation n° 1
Faire preuve de vigilance pour repérer les tentatives d'escroquerie

L'Observatoire recommande aux utilisateurs intéressés par des solutions de paiement par crypto-actif de vérifier les autorisations réglementaires des fournisseurs et des crypto-actifs utilisés. Les crypto-actifs non autorisés dans l'Union européenne doivent être refusés.

L'Observatoire rappelle également ses recommandations générales de sécurité : ne pas réagir face aux contacts non sollicités, ne pas cliquer sur des liens sponsorisés, mais se rendre par ses propres moyens sur le site internet, ne jamais valider d'opérations dont on n'est pas à l'origine, etc.

Les autorisations réglementaires peuvent être vérifiées sur le site de l'Autorité européenne des marchés financiers (AEMF) pour les prestataires de services sur crypto-actifs (PSCA), et sur le site de l'Autorité bancaire européenne (ABE) pour les prestataires de services de paiement (PSP). Les listes noires [33] de l'ACPR et de l'AMF permettent également d'identifier des fournisseurs étant en exercice illégal d'activité.

Recommandation n° 2
Veiller à sécuriser ses données sensibles de paiement

L'Observatoire recommande aux utilisateurs finaux de solutions de paiement par crypto-actif de protéger leurs clés privées stockées, selon le type de portefeuille (physique ou numérique) [34] :

- en conservant l'appareil dans un endroit sécurisé, en n'enregistrant pas la phrase de récupération en ligne, et en s'assurant d'avoir un mot de passe robuste ;
- en s'authentifiant fortement à la plateforme d'échange ou au fournisseur de portefeuilles autohébergés ;
- en cas de demande par téléphone ou par courriel par un tiers, en ne communiquant jamais ses informations sensibles de paiement ;
- en mettant à jour régulièrement les appareils et moyens de stockage des clés privées vers les versions actualisées plus sécurisées de ces appareils et moyens de stockage ;
- en se protégeant contre les connexions non sécurisées, comme les réseaux publics non sécurisés, et en utilisant une connexion internet sécurisée et un réseau privé virtuel (VPN) visant à protéger les données sur internet et permettant de naviguer anonymement.

Recommandation n° 3
Privilégier les paiements par des actifs régulés tels que les jetons de monnaie électronique

L'Observatoire recommande aux utilisateurs et commerçants intéressés par ces solutions de privilégier des crypto-actifs émis par des acteurs régis par le règlement MiCA, tels que les jetons de monnaie électronique, pour les paiements du quotidien, afin de bénéficier de la sécurité attachée au régime réglementaire encadrant ces actifs.

Recommandation n° 4
Pour les commerçants, privilégier l'utilisation de QR codes dynamiques

Les QR codes statiques mis à disposition de la clientèle présentent un risque de fraude (fraude au *quishing*). Par conséquent, les QR codes statiques pour les systèmes de caisse ne disposant pas d'affichage numérique semblent moins sécurisés.

RECOMMANDATIONS À L'ATTENTION DES ACTEURS DU MARCHÉ DES PAIEMENTS PAR CRYPTO-ACTIF

L'Observatoire renvoie, en premier lieu, aux **propositions [35] publiées en 2025 par le « Groupe de travail sur la certification**

des *smart contracts* », sous l'égide du Forum Fintech ACPR-AMF, en matière d'audits, de gouvernance et de réglementation des contrats intelligents (*smart contracts*).

L'Observatoire renvoie également les prestataires de solutions de paiement par crypto-actif à ses recommandations de 2023 pour anticiper les risques quantiques (inventorier les dispositifs de sécurité, tester des algorithmes post-quantiques, et établir une feuille de route pour anticiper les risques liés à l'informatique quantique) [36].

Recommandation n° 5
Garantir un niveau de protection équivalent, par les acteurs régulés ou non, en mettant en œuvre les règles d'authentification forte au sens de la DSP2 pour toutes les solutions de paiement par crypto-actif, y compris les crypto-actifs autres que les EMT

Les paiements par crypto-actif nécessitent l'intervention de multiples acteurs. En suivant strictement les principes de sécurité issus de la deuxième directive européenne sur les services de paiement (DSP2), l'Observatoire rappelle qu'il est essentiel d'authentifier fortement le processus de paiement (accès au compte ou au portefeuille, initiation d'un paiement à distance, opérations sensibles comme le changement de mot de passe, d'IBAN ou d'appareil de confiance).

A fortiori, il est important d'appliquer ces règles à l'ensemble des acteurs proposant des solutions de paiement par crypto-actif, qu'ils soient régulés ou non, compte tenu des actifs proposés (EMT et autres crypto-actifs) pour les opérations de paiement par carte adossée à des crypto-actifs ou par portefeuille de crypto-actifs, ainsi que la protection des données sensibles de paiement.

Recommandation n° 6
Assurer un niveau de surveillance en temps réel des paiements par crypto-actif équivalent à celui mis en œuvre dans le cadre des paiements traditionnels

L'Observatoire invite les acteurs de la chaîne des paiements par crypto-actif à assurer un degré de surveillance de ces paiements équivalent à celui appliqué aux paiements traditionnels (par l'évaluation du niveau de risque individuel de chaque transaction notamment), afin de lutter efficacement contre la fraude.

Recommandation n° 7
Privilégier l'utilisation de portefeuilles intégrant la méthode MPC de gestion des clés privées

Le portefeuille utilisant la technologie de calcul MPC est un mécanisme qui permet de renforcer significativement la sécurité opérationnelle des paiements par crypto-actif. L'utilisation d'une telle méthode intégrée à un portefeuille permet donc d'éviter la vulnérabilité liée à l'utilisation de portefeuilles classiques.

Recommandation n° 8
Avant de faire appel à une nouvelle chaîne de blocs, il est nécessaire de procéder à une analyse de risques. Cette surveillance doit également s'opérer dans la durée, notamment lorsque la chaîne de blocs évolue.

Afin de s'assurer de la sécurité de l'infrastructure, l'Observatoire recommande aux émetteurs de crypto-actifs souhaitant faire appel à une nouvelle chaîne de blocs dans le cadre de leurs activités, d'effectuer, en amont, une analyse des risques, et de s'assurer que la chaîne présente un haut degré de sécurité. Il est également important d'auditer régulièrement la chaîne de blocs, car celle-ci est vouée à évoluer dans le temps au gré des mises à jour fonctionnelles. Ces analyses doivent naturellement étendre leur périmètre aux processus externes à la chaîne de blocs, qui visent à en améliorer le fonctionnement.

33 Assurance Banque Épargne Infoservice : « Listes noires des autorités ».

34 Plateforme MesServicesCyber, Anssi, « Recommandations relatives à l'authentification multifacteur et aux mots de passe ».

35 Ces propositions visent en premier lieu les activités décentralisées, mais peuvent aussi s'appliquer plus largement aux activités centralisées.

36 Rapport annuel de l'OSMP 2023, chapitre 3 (pages 73-90) : « L'informatique quantique et la sécurité des systèmes de paiement par carte bancaire ».

Éditeur
Banque de France

Directeur de la publication
Érick Lacourrège
Directeur général des Moyens de paiement
Banque de France

Rédacteur en chef
Julien Lasalle
Adjoint au directeur des études et de la surveillance des paiements
Banque de France

Secrétariat de rédaction
Pierre Bienvenu, Clément Bourgeois, Trân Huynh,
Fatih Kurt, Armand Thomas et l'ensemble des membres
du groupe de travail Veille technologique de l'OSMP 2025

Réalisation
Studio Création
Direction de la Communication

Contact
Observatoire de la sécurité des moyens de paiement
Code courrier : S2B-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Dépôt légal
Septembre 2026
ISSN 2557-1230 (en ligne)
ISSN 2556-4536 (imprimé)

Internet
www.observatoire-paiements.fr

www.banque-france.fr