OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

Security of payments using crypto-assets

ANNUAL REPORT 2025: EXTRACT

BANQUE DE FRANCE
EUROSYSTÈME

www.observatoire-paiements.fr

OBSERVATORY FOR THE SECURITY OF PAYMENT MEANS

Security of payments using crypto-assets

ANNUAL REPORT 2025: EXTRACT

Advance publication of a study from the *2025 Annual Report of the Observatory for the Security of Payment Means,* due for release in the second half of 2026

APRIL 2026

SECURITY OF PAYMENTS USING CRYPTO-ASSETS

1 Introduction

The emergence of new technologies, such as distributed ledger technology[1] (DLT), has led to the development of new types of financial assets. These include "crypto-assets", which can be exchanged between economic players and serve as a means of settling[2] retail and financial transactions without, in principle, resorting to cash or cashless means of payment or traditional market infrastructures. These crypto-assets form the cornerstone of decentralised finance (DeFi), which aims to dispense with traditional centralised finance and payment channels. This decentralisation means that transaction monitoring, decisions and validations are carried out by a network of participants, according to mechanisms defined by the underlying network, without a single central authority.

A crypto-asset is defined as a digital representation of value or rights that is able to be transferred and stored electronically using DLTs, such as blockchain, or similar technology. Their issuance and distribution are governed in the European Union by the MiCA Regulation.[3] For the purposes of this study, we consider two types of assets:

- "first-generation" crypto-assets, such as Bitcoin and Ether, which are not pegged to a reserve of assets and whose value is highly volatile – linked to supply meeting demand – compared with legal tender currencies;
- "second-generation" crypto-assets, or "stablecoins", which were created in an attempt to overcome this volatility and are often pegged to a traditional financial asset such as a currency, commodity or security, or basket of assets (a stock market index, for example). When designed for use as a settlement asset, they are generally pegged at a 1:1 ratio to a legal tender currency. In accordance with the MiCA Regulation and the clarifications provided by the European Banking Authority (EBA), they therefore qualify as "electronic money tokens" (EMT)[4] and are classified as electronic money units for regulatory purposes (in particular, the second European Payment Services Directive – PSD2 – and the second Electronic Money Directive – EMD2).[6]

From an infrastructure perspective

From an operating perspective, crypto-asset transactions are recorded in a blockchain[7] and distributed via a decentralised and generally public network, whose purpose is to group, secure and timestamp those transactions cryptographically to guarantee their traceability and integrity. Taken individually, certain aspects of these technologies resemble those used to secure traditional payments. However, when combined with blockchain technology, they can operate in a fully decentralised manner without a trusted third party to maintain a reference account. In fact, every participant, or "node", in the blockchain has an identical copy of the ledger of transactions, making attempts at falsification more complex.

From a players' perspective

In practice, direct access to the blockchain requires information technology (IT) skills and resources that are generally beyond the reach of traditional retail payment users (merchants or consumers). As a result, the implementation of retail payment solutions using crypto-assets requires specialised intermediaries, which then delegate the execution of crypto-asset unit exchanges through the blockchain.

1 A "distributed ledger" is an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism (Article 3 of the European Markets in Crypto-Asset Regulation – MiCAR).

2 The use of crypto-assets for settlement purposes in the purchase of other crypto-assets (including unique and non-fungible crypto-assets or real-world assets represented in the form of tokens) is excluded from the scope of the study.

3 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

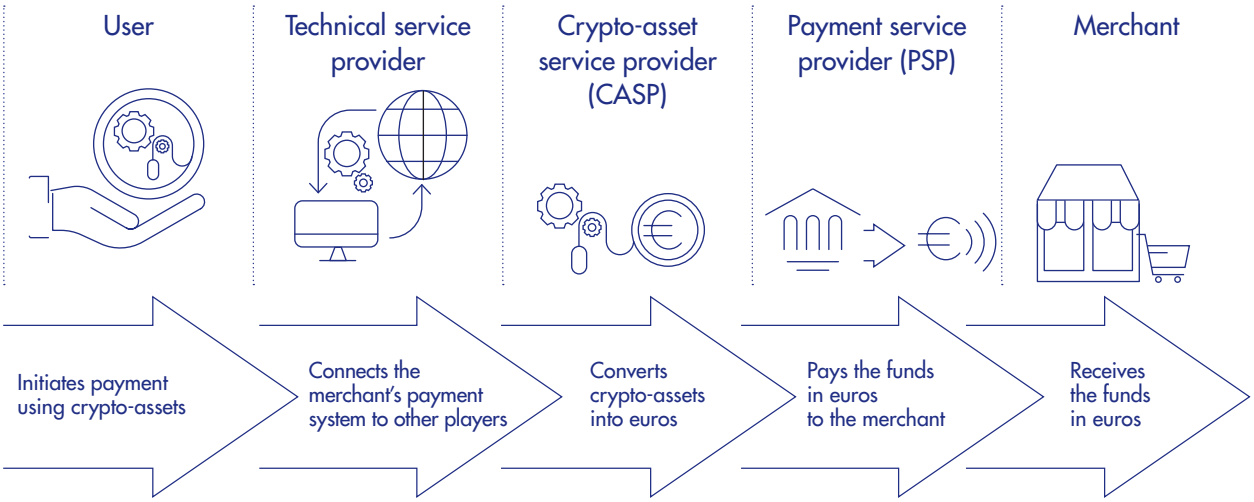
4 EMT: "e-money token" issued by an electronic money institution (EMI) or credit institution (CI).

5 Article L. 315-1 of the French Monetary and Financial Code (CMF I. and II): "Electronic money is a monetary value stored in electronic form, including magnetic form [...] and electronic money units are said to be units of value."

6 European Directive (EU) 2015/2366 on payment services (PSD2) and Directive 2009/110/EC on electronic money (EMD2).

7 For further information, see: *"La blockchain"*, Banque de France, ABC de l'Économie, *L'Éco en Bref*.

D1 OVERVIEW OF THE PLAYERS INVOLVED IN PAYMENTS USING CRYPTO-ASSETS



Source: Observatory for the Security of Payment Means.

Throughout the crypto-asset payment journey, various players intervene to facilitate the payment, from the end user to the merchant that accepts them as a method of payment. Thus, in order to bring together the various payment using crypto-assets stakeholders, players such as crypto-asset issuers, exchange platforms[8] and banking institutions, which are notably in charge of transferring the transaction amount in euro to the merchant, can be involved.

Bridges with the "traditional" payment sector exist

In almost all cases, merchants prefer to receive payment in legal tender currency, i.e. euro, which requires the crypto-assets used by the payer to be converted before the proceeds of the conversion are passed on to the merchant. Various conversion options are available, depending on the type of payment using crypto-assets – QR codes,[9] payment cards or crypto-asset wallets – and each involves a mix of crypto-asset services and traditional payment services.

The objectives of this study

This study falls within the remit of the *Observatoire de la sécurité des moyens de paiement* (OSMP – Observatory for the Security of Payment Means) as it focuses on an analysis of the security of retail payments using crypto-assets in France.

This study is intended to provide an overview of payment using crypto-assets solutions in France following the entry into force of the European MiCA Regulation (MiCAR), to identify the security issues specific to payment using crypto-assets, and given this context, to present the recommendations the OSMP considers appropriate.

Other risks[10] associated with crypto-asset holdings or use (market, credit, liquidity or money-laundering risks) are therefore not discussed as part of this study. However, any players intending to hold or trade crypto-assets, or more broadly, offer crypto-asset-related services, should take them into consideration. Similarly, neither the strictly legal aspects of payment using crypto-assets,[11] nor the tax implications involved, will be addressed in this study.

2 A typology of payments using crypto-assets

Technically, first-generation crypto-assets such as Bitcoin can be used to make payments but in practice, their value volatility and the fees and delays associated with each transaction mean that they are unsuitable for everyday payments. Consequently, the following analysis primarily concentrates on stablecoin payments and their use cases, while also marginally touching on certain use cases for first-generation payments using crypto-assets. Since merchants prefer in practice to be paid in euro, using stablecoins notably means that the exchange risk and volatility associated with other crypto-assets when converting to a legal tender currency are more limited.

It is important to note from the outset that **crypto-assets are currently very rarely used in retail payments in France**. In fact, less than 3% of French people[12] surveyed in 2023 claimed to have already used crypto-assets for payment purposes. Moreover, the number of referenced retail businesses directly accepting payments using crypto-assets in France in 2025 was very low. For example, approximately 300 out of a total of 300,000 points of sale – 0.1% – accept Bitcoin.

Furthermore, crypto-assets, including stablecoins, are used to buy and sell other crypto-assets, but in practice are only marginally used to purchase traditional goods and services. Nevertheless, leaving aside retail payments made in France, the use of stablecoins, particularly those regulated under MiCAR, is growing, mainly for transactions on financial markets, for cross-border payments between professionals and for cash management, including at group level.

2.1 Point-of-sale payments

From a practical perspective, instruments similar to those available for traditional payments are used for point-of-sale payments using crypto-assets. **Payment initiation** is made either via a merchant's electronic payment terminal, which generates a QR code containing the transaction information, or via a customer's payment card, be it the card itself or integrated into their mobile phone. Whatever the case, the crypto-asset **payment acceptance** solution can be integrated into the cash register system or provided on a device such as a tablet or phone, used as a mobile payment solution (SoftPos – Software point of sale).

In the case of a point-of-sale payment with a QR code, customers first scan the QR code generated by the merchant's payment terminal. Depending on the options offered by the merchant, customers then choose (i) their exchange platform, (ii) their crypto-asset wallet (if they have several), and (iii) the crypto-asset they wish to use for payment. In the next step, the payer validates the transaction with the exchange platform or EMT issuer, which then transmits it to the blockchain network. Lastly, the transaction is confirmed and the sale is finalised. This is followed by a conversion phase, which has no impact on the customer's payment journey, during which the payment passes through a payment gateway, in charge of establishing the link between crypto-assets and traditional banking channels (such as SEPA). The exchange platform, or EMT issuer, converts the crypto-assets into a legal tender currency (euro), and the amount is then paid in euro to the merchant through a payment service provider.

In the case of a point-of-sale payment with a payment card, the payment is made by placing a physical or virtual card in contact with a payment terminal. Most cards are preloaded with crypto-assets or are connected to a crypto-asset wallet. Several options for the crypto-asset to be used for payment are available. In principle, the user sets a default choice for future transactions but that choice may automatically switch to another crypto-asset when the balance of the default asset does not cover the entire payment. The conversion into a legal tender currency then takes place via payment gateways on an exchange platform or another crypto-asset service provider (CASP), in the same way as payments with a QR code. Lastly, the transaction is carried out through traditional card payment networks until the merchant receives the funds through the intermediary of their payment service provider (PSP).

For both types of crypto-asset point-of-sale payment solutions, an internet connection is most often required to validate the transaction. However, it is sometimes possible to pay offline – without a direct internet connection – depending on the chosen payment method[13] through the use of NFC[14] technologies or QR codes.

2.2 Remote payment transactions

Remote payment transactions using crypto-assets can be made as an e commerce payment through a traditional payment method (such as a card, bank transfer, or from an electronic money account), either directly from the merchant's website or from a payment link generated by the merchant. The option to pay using crypto-assets becomes available alongside other possible options when prompted to choose the payment method. The payment

8 These exchange platforms convert the crypto-assets held in a user's crypto-asset wallet.

9 Quick Response (QR) code payment is a digital payment solution whereby payers scan a two-dimensional code with their smartphones to initiate a transaction.

10 "*Crypto-actifs: l'AMF appuie l'appel à la prudence lancée par l'ESMA à destination des investisseurs individuels*", AMF (18 December 2024). It is important to bear in mind that crypto-assets are very risky because they generally offer little protection and are generally less regulated than most other types of assets, with some players sometimes unregulated.

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

12 "*Quel avenir pour le monde des crypto-actifs?*", Banque de France, 17 October 2024.

13 Self-custody wallet, hard wallet or specific payment cards.

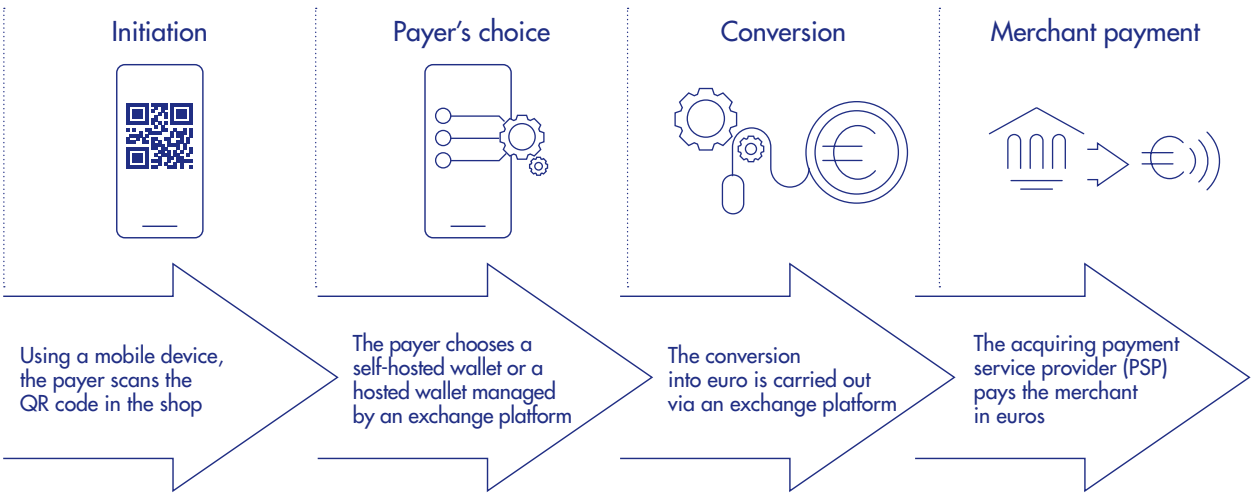
14 Near Field Communication technology enables very short-range data payload sharing between compatible devices.

then proceeds as described above, with the choice of asset in the electronic wallet, the completion of the transaction, and then the conversion to pay the merchant in a legal tender currency.

2.3 Wallet-to-wallet payments

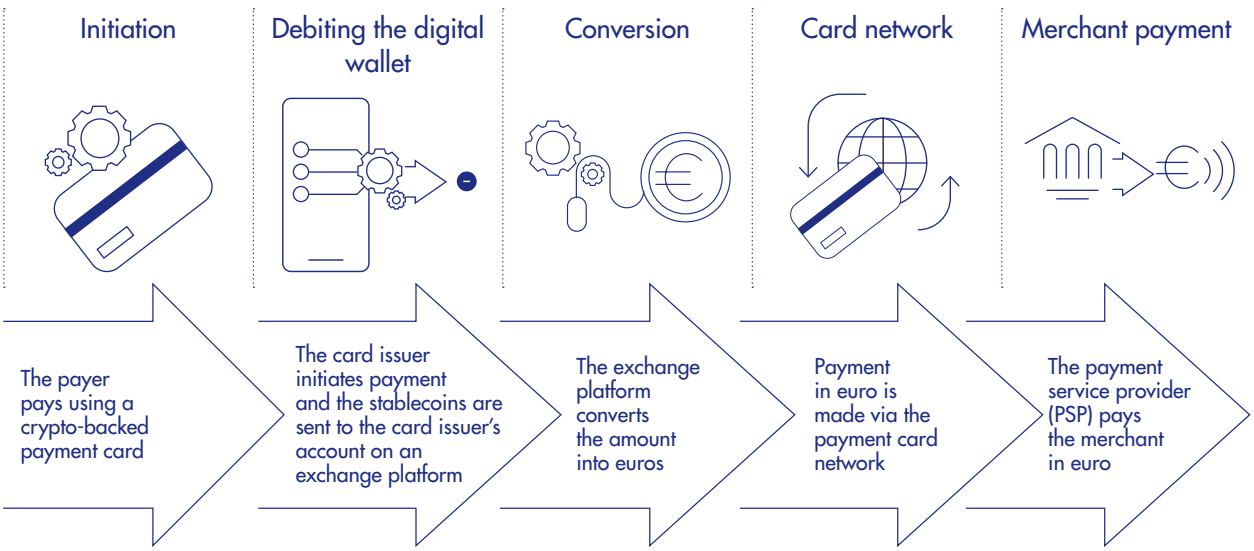
There is an alternative – albeit very rarely used – payment method in which both the user and the merchant have a crypto-asset wallet. In this scenario, payment is made directly from one wallet to another, using crypto-assets without conversion into legal tender currency. It can be applied in both remote and point-of-sale payments but is virtually non-existent in France. The risks to the user in the case of a payment made directly from wallet to wallet are heightened when the wallets are self-hosted (non-custodial wallets),[15] or a payment is made using non-EMT crypto-assets.

D2 POINT-OF-SALE PAYMENT FLOWS USING A QR CODE



Source: Observatory for the Security of Payment Means.

D3 POINT-OF-SALE PAYMENT FLOWS USING A PAYMENT CARD



Source: Observatory for the Security of Payment Means.

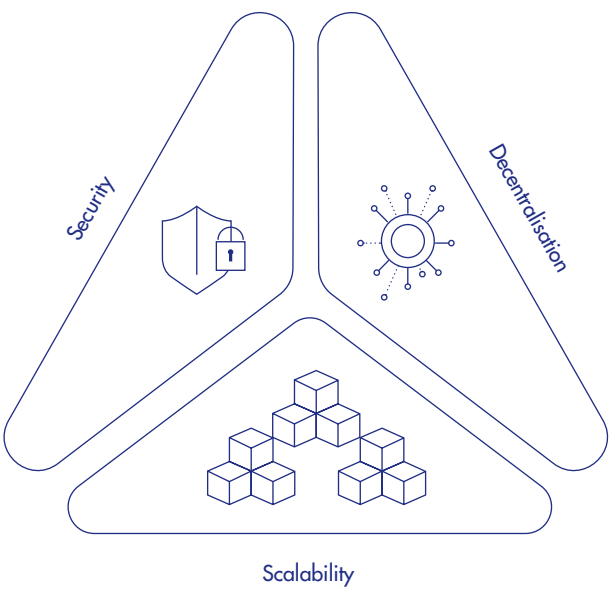
3 The underlying technical functionality

The principle of blockchain is structured around an IT infrastructure implementing technical protocols that enable the entire system to function.

The two main categories of blockchains – permissioned and permissionless – are determined by their mode of participation (often private, and often public, respectively). Technically, both function identically but what distinguishes them is their access. In private blockchains, transactions are only visible to participants who have permission to access them. Access is therefore limited and, as a result, there is only partial transparency. On the other hand, when the blockchain is public, the transactions are visible to all and are regarded as immutable, and network fees can sometimes be high.

At the design stage of a blockchain, the main objectives pursued are (i) network security, (ii) decentralisation (control by multiple participants), and (iii) scalability (the system's capacity to handle more transactions more quickly and at lower cost). These three objectives are difficult to reconcile, and make up a kind of "trilemma". The functioning of blockchains has therefore evolved in recent years to strike an optimal balance depending on market uses and expectations.

D4 THE BLOCKCHAIN TRILEMMA



Source: Observatory for the Security of Payment Means.

3.1 Native blockchains

Originally, the blockchain was based on a first layer – "Layer 1" – which allows transactions to be recorded directly "on-chain". It employs consensus mechanisms[16] to guarantee process security and decentralisation. These mechanisms consist of a network of nodes[17] that use various protocols[18] to agree on the validity of transactions without the intervention of a central authority. This so-called blockchain "infrastructure" is designed with security, governance, consensus and execution features.

The structure of the underlying technology can be broken down into three main components:

- the **network**, which consists of several computers or servers – nodes – that execute an algorithm to secure the system by receiving transactions, validating them according to the rules of the protocol used, and storing the blocks;
- the **blocks**, which comprise a set of transactions and which can vary in number depending on the chain used; and
- a **chain**, which links the blocks end-to-end through a cryptographic[19] hash, which consists of an unalterable digital fingerprint that secures the transaction (in practice, the data contained in the previous block are encrypted and thus immutable).

Execution time can be long and costly depending on several factors:

- the number of computers validating the transaction – transaction processing speeds vary depending on the network and the number of active validators;
- fees – the "nodes" prioritise transactions with higher network fees (as this is how the node validators are remunerated), more commonly known as "gas fees".
- network congestion – as the number of active nodes[20] is fixed, transactions that accumulate may be put on hold until a new block to contain them becomes available.

15 In this case, private keys are stored locally on the device.

16 A pre-defined process, through which the transaction is completed.

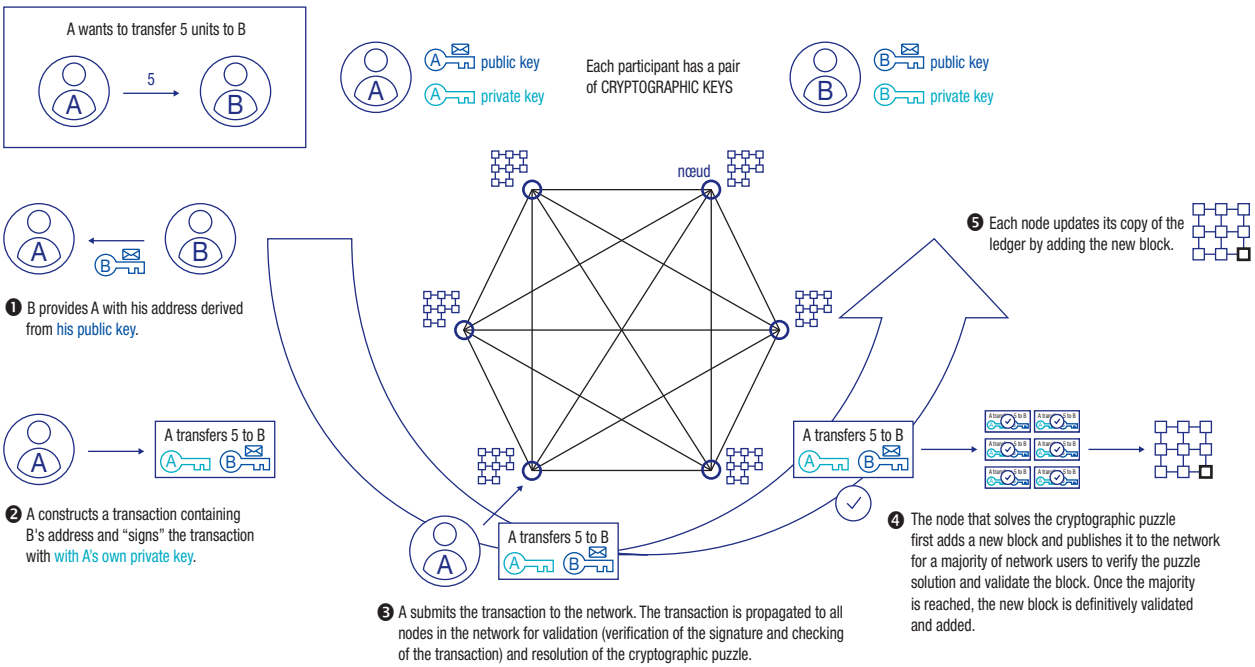
17 A network made up of machines/computers that contribute to the storage, validation/verification and exchange of transaction information.

18 Proof of work or proof of stake.

19 Cryptographic security is built into the blockchain protocol, so the end user has a private key to sign the transaction. Signature verification is a decentralised process, using a public key.

20 For example, for the main networks, the number of nodes is now up to 2,500 for Bitcoin, 1,400 for Ethereum, 5,000 for Solana, and 2,000 for Polygon.

D5 VALIDATION OF A TRANSACTION IN A BLOCKCHAIN WITH PROOF OF WORK



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

⇨ For low value transactions, network fees are not negligible and the transaction can take around ten minutes or longer to be validated, with a risk of network congestion. For these reasons, Layer 1-based payments using crypto-assets appear unsuitable for everyday purchases of goods or services, and are therefore not – or very rarely – used in this regard. This technical complexity notably explains the marginal – if not almost non-existent – use of crypto-assets in the strict sense among the payment solutions offered by merchants in France. They are therefore used almost exclusively as speculative assets for investment ends.

3.2 Application-specific blockchains

The introduction of an additional layer of blocks, known as "Layer 2", is intended to accelerate and improve the entire blockchain's performance. To do this, transactions are processed off-chain and then validated in Layer 1. The transactions are thus aggregated and processed in bulk, increasing the number of transactions that can be handled and reducing the associated costs.

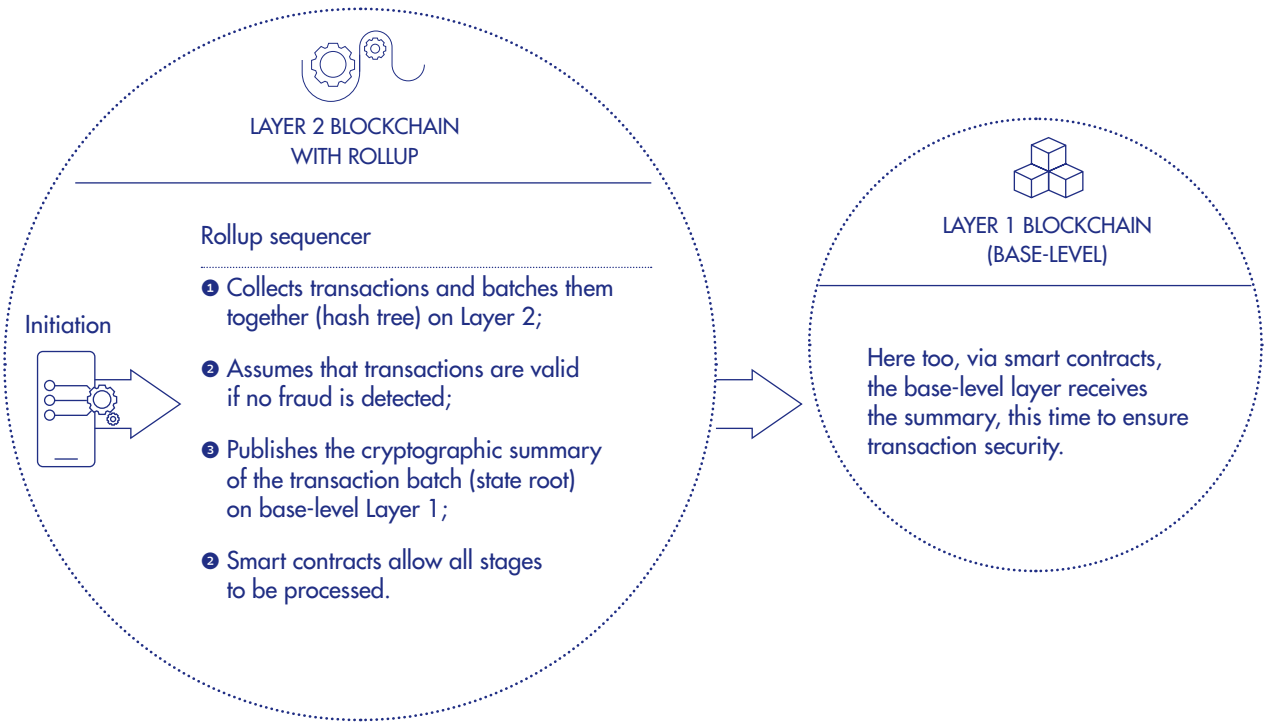
Layer 2 is constantly evolving with the pace of innovation, and several models currently exist. For example, the "optimistic rollup" protocol operates on the assumption that transactions are valid if the detection mechanisms identify no evidence of fraud. The sequencer, which is an operational component of rollups, collects, orders and executes several operations outside the blockchain, thus processing transactions more quickly, and thereby reducing fees. The sequencer batches the transactions together.[21] In this case, a summary of all transactions is published on Layer 1 and the transactions are not immediately verified on this Layer 1 (a detailed verification may take place retrospectively during a dispute period in the event of fraud, for example). On the Layer 2 blockchain, application-based "smart contracts"[22] allow all stages to be processed, and control "smart contracts" on the Layer 1 base chain then ensure security. Another method, used by Zero-Knowledge Rollups (ZK Rollups),[23] further secures operations by generating cryptographic proofs to ensure their validity. These proofs are thus recorded on Layer 1 without revealing the details of the transactions.

A "Layer 3" also emerged very recently. Layer 3 acts as an application layer that facilitates interoperability between layers. It is designed to connect blockchain Layers 1 and 2 with inherent applications and services, without the intervention of a third party.

These additional layers, which have been overlaid on the original blockchain, play an essential role in the development of these new technologies. They underpin the ecosystem's growth possibilities and ensure the interaction between its components.

⇨ Interoperability is an issue that is intrinsic to the technological aspects. Each blockchain network has its own standards, necessitating the use of gateways and therefore creating a first potential point of vulnerability in the payment chain.

D6 ILLUSTRATION OF THE "ROLLUP", A LAYER 2 BLOCKCHAIN PROTOCOL



Source: Observatory for the Security of Payment Means.

4 The security challenges

Payments using crypto-assets are exposed to two types of risk: (i) the "classic" risks affecting the use of traditional means of payment; and (ii) the risks more specifically associated with the use of crypto-assets, which relate to the inherent technical characteristics of these new settlement assets.

4.1 The "classic" risks

It may not be unique to payments using crypto-assets, but it is important to note from the offset that online scams and fraud involving crypto-assets have increased, and should therefore be a major concern for potential users.

21 They are grouped and organised according to a hash tree or Merkle tree. This is a data structure used in cryptography to reduce the amount of data that needs to be stored in a blockchain for verification purposes. The root hash summarises all the data contained individually in each transaction processed within the same batch.

22 An autonomous programme deployed on a blockchain that automatically executes predetermined rules.

23 The *Report on Decentralised Finance (DeFi)*, European Union Blockchain Observatory and Forum, 24 May 2022, describes a Zero-Knowledge (ZK) rollup as "a scaling solution that executes transactions off-chain and then publishes a cryptographic proof of validity on Layer 1. This proof guarantees the compliance of transactions without disclosing their data, reducing the amount of information to be published on the main blockchain".

In general, when payments using crypto-assets are made through the use of a traditional payment card, users are exposed to the risks associated with card transactions. In terms of security, ISO standards[24] are applied and cryptographically protected data fields are often used. In addition, payment data is encrypted using symmetric and asymmetric encryption algorithms (respectively, Advanced Encryption Standard [AES] and RSA [named after its three inventors] algorithms). Furthermore, the payment processing chain is certified under the Payment Card Industry Data Security Standard (PCI-DSS). However, not all current encryption methods are post-quantum and may therefore prove vulnerable to attacks.

⇨ Measures to adapt to post-quantum encryption must therefore be implemented – in accordance with the recommendations[25] already issued by the OSMP – to prevent this risk to operational resilience.

Similarly, the use of QR codes can also be a vulnerability, notably because fraudsters are able to falsify them (quishing). In this case, the fraudster replaces an authentic QR code with their own fake code in order to receive payments that should otherwise go to a merchant. This method has already been observed in the context of the use of this payment initiation mechanism. Some merchants provide their customers with a static QR code, though this is a factor of risk because static QR codes function indefinitely and can therefore be more easily falsified.

⇨ Dynamic QR codes, on the other hand, expire, thereby reducing the associated risk of fraud.

Generally speaking, the sheer number of players participating in the crypto-asset payment process, which was discussed above, affects the fluidity of the act of payment (and therefore lengthens the time it takes). Moreover, the multiplicity of stakeholders compromises the resilience of the payment chain by introducing an equal multiplicity of potential points of vulnerability.

Furthermore, these payment solutions are less resilient than traditional means of cashless payment. For example, a recent outage at a major cloud provider[26] caused service interruptions that affected several crypto-asset players. The malfunction impacted access to blockchain networks, payment application programming interfaces (APIs) and users' electronic wallets. Resilience also depends on the choice of hosting provider. Concentration around a limited number of critical service providers – that is, services that can influence the security and performance of the system – can indeed give rise to difficulties when data is replicated on two sites that both belong to the same cloud provider.

⇨ Strengthening the Emergency and Business Continuity Plan is therefore essential in light of the potential operational resilience risks that are significantly exacerbated by the use of crypto-assets as a means of payment and by the huge number of players involved in the payment journeys.

4.2 In addition to the "classic" risks, there are new risks specific to the use of crypto-assets

4.2.1 Blockchain security risk

Blockchains are based on the three principles of cryptography, decentralisation and consensus, which aim to intrinsically ensure their security qualities. However, these native principles are certainly not infallible, especially in the current context of layer accumulation, which aims to optimise blockchain functionality.

The security of blockchains therefore depends heavily on the robustness of the underlying technical infrastructure and protocols. The reliability of nodes, the resilience of cloud providers, the security of APIs and the dependability of "smart contracts" are all critical factors to take into consideration.

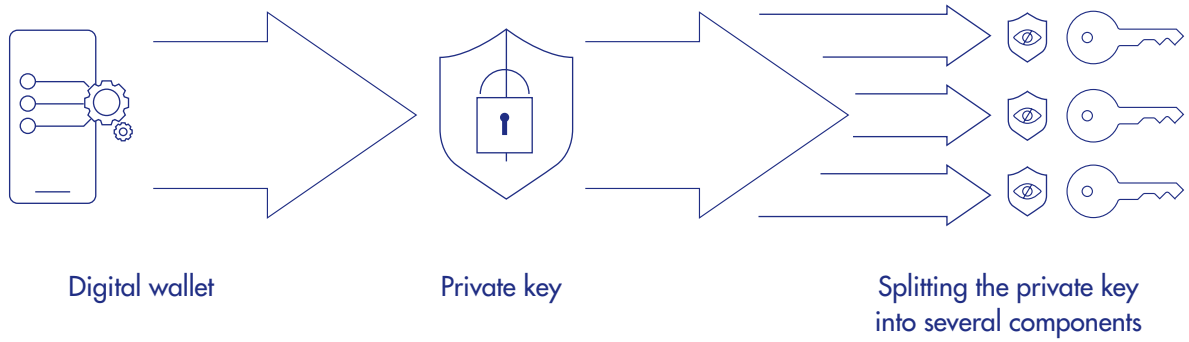
⇨ Given this context, a thorough assessment of the operational robustness of technical components is essential to ensure the security of payments using crypto-assets.

4.2.2 The risk of loss/theft of private keys and data leaks

There are different types of crypto-asset wallets. The two main types are physical (hard wallets) and digital (hot wallets or software wallets). Physical wallets have private keys stored on a medium such as a USB stick or secure chip. Digital wallets have private keys stored on a device connected to the internet, in the case of a non-custodial wallet, or online on a remote server, in the case of a custodial wallet.[27] Asymmetric keys are used to secure digital wallets, with a private key used to sign the transaction and a public key used to receive the funds. Consequently, for a purchase, the end user of the blockchain will have a private key to sign the transaction on their digital wallet, while the public key – similar to the bank details of a traditional account – comprises the address for the reception of funds. This public key can, for example, be communicated via the QR code presented by the merchant to the customer.

⇨ Private keys, whether stored on a physical or a digital wallet, constitute sensitive payment data and as such must be protected. They must therefore be secured in order to prevent irreversible loss of access to

S7 WALLET THAT USES A SECURE MULTI-PARTY COMPUTATION (MPC) TECHNIQUE



Source: Observatory for the Security of Payment Means.

crypto-assets or avoid their being compromised by a malicious third party to seeking carry out unauthorised transactions. This enhancement of security should notably include regular updates of devices and storage media for private keys to incorporate the latest versions, as well as protections against unsecured connections, such as unsecured public networks, by using a virtual private network (VPN), for example.

Furthermore, the fraud techniques used to obtain private keys, which give access to crypto-asset wallets and therefore the ability to make payments, are similar to those used for traditional payments: phishing, smishing, fake websites, etc.

⇨ However, more secure versions do exist, such as wallets that incorporate either multi-signature protocols or secure multi-party computation (MPC) techniques. A wallet using an MPC technique is a cryptographic solution more suited to retail payments, in which the entire private key is no longer stored in one single place. It is split by multi-party computation protocols between the payer, the service provider and, potentially, a trusted third party. Consequently, compromising the private key becomes more difficult.

4.2.3 The risks associated with smart contracts

Another potential point of vulnerability lies in the fact that payments using crypto-assets are most often made via systems that are automatically executed when predetermined terms and conditions are met at the blockchain level, known as "smart contracts". In practical terms, these are computer codes written in a programming language specific to the blockchain used. The objective is to predetermine the conditions for the execution of operations, whether they involve issuing crypto-asset units or other transactions, and to define the roles and functions of the parties involved. For example, with these smart contracts it is possible to make the execution of a payment conditional on the fulfilment of an external condition, such as the provision of funds in an account or the authorisation of a transfer, and to schedule the execution of recurring transactions. However, smart contracts can be modified during an external hack using conventional cyberattack methods, for example, or through internal fraud carried out by an individual able to act within the entity operating the smart contract. Once the contract has been modified, the fraudster can then commit a wide range of fraudulent activities: gaining access to asset portfolios, making fraudulent payments, etc.

The Open Web Application Security Project (OWASP) – an international non-profit organisation dedicated to improving web application security – has identified the top ten vulnerabilities found in smart contracts and has drawn up several security recommendations in response.[28]

24 Standards defined by the International Organization for Standardization (ISO) and applicable to products and services.

25 Chapter 3 (pages 37-53) of the *Annual Report of the Observatory for the Security of Payment Means 2023*: "Quantum computing and the security of bankcard payment systems".

26 IT service provider (infrastructure hosting services, data hosting services, etc.).

27 Private keys are stored on third-party servers, such as exchange platforms.

28 On the OWASP Smart Contract Security website.

Illustrations of the main vulnerabilities of "smart contracts"

1. "Reentrancy attacks": these can lead to the embezzlement of funds by a fraudster who manages to execute a programme function several times before the smart contract updates its internal state to reflect the completion of the transaction (as in the PenPie Hack in 2024).

2. Access control failure: the fraudster manages to access programme functions that should only be accessible to the administrator, such as refunds, in order to misappropriate funds (as in the Bybit Heist in February 2025).

3. A flaw in the overflow check within the liquidity calculation function: a flaw in the smart contract that allows a hacker to trick the programme into believing that more liquidity is being added than is actually the case. As a result, the smart contract price calculations become distorted, allowing the attacker to withdraw more assets than have actually been contributed (as in the Cetus Hack in May 2025).

Smart contract security is therefore a key challenge. As such, players have implemented certain best practices, such as having the smart contract audited by an independent third party, some of which are certified by the *Agence nationale de la sécurité des systèmes d'information* (ANSSI – the French national cybersecurity agency) as 'information system security audit providers' (Passi),[29] which attests to their expertise in cybersecurity.

⇨ Furthermore, the *Autorité de contrôle prudentiel et de résolution* (ACPR – the French Prudential Supervision and Resolution Authority) and the *Autorité des marchés financiers* (AMF – the French Financial Markets Authority) have published a working group report on smart contract certification (*Rapport du groupe de travail sur la certification des contrats intelligents*). It sets out several suggestions to guide (i) the definition of certification standards for smart contracts, including the broader security principles that these could encompass, (ii) the use of existing audit methods in the context of this certification and the bodies and resources likely to implement them, and (iii) regulatory approaches that could be incorporated into a potential certification scheme.

4.2.4 Real-time monitoring of Layers 1 and 2

In addition to the risks associated with the primary blockchain (Layer 1), transactions carried out within Layer 2 must also be subject to monitoring, as they form external circuits to the primary blockchain, the results of which are then fed back into it. The bridge between Layer 1 and Layer 2 is thus also a potential point of vulnerability.

⇨ Payments using crypto-assets should therefore be monitored in real time, in the same way as traditional payments, in order to ensure operational security to counter attacks and detect fraudulent transactions, and thereby combat fraud effectively.

5 Compliance challenges

5.1 Challenges related to the security of the payment journey

Payment solutions using crypto-assets must comply with the regulatory requirements regarding payment journey security, which form the basis of this study, with all other regulatory aspects excluded. Application of the rules set out in the second European Payment Services Directive (PSD2) is therefore mandatory for crypto-assets, which are classified as "electronic money tokens" (EMTs) and thus treated as funds. However, their application is not strictly mandatory for payment solutions based on crypto-assets that are not classified as funds. These include first-generation crypto-assets or "asset-referenced tokens" (ARTs). As a result, certain unregulated players offer payment solutions using crypto-assets other than regulated EMTs, which therefore present a non-negligible risk to users.

⇨ Based on the "same activity, same risk" principle, it is recommended that all players, regulated or not, comply with these rules for their crypto-based payment solutions, regardless of the legal classification of the crypto-asset itself. This particularly applies to the requirements for strong transaction authentication.

The security regulations set out in PSD2 apply to crypto-assets classified as EMTs, in particular those relating to strong customer authentication (SCA)[30] for online payments, PIN code use for card transactions exceeding EUR 50, and biometrics for mobile transactions. Beyond payments, crypto-asset service providers (CASPs) must also ensure strong end-user authentication to make access to crypto-asset wallets and the execution of sensitive operations (password or IBAN changes, registration of a new trusted device, etc.) more secure.

⇨ In this regard, the review of the PSD3/PSR legislative package currently underway and its potential regulatory implications for players in the crypto-asset payment chain will have to be monitored very closely, as it is important to ensure that all players in the sector comply with the security requirements established by the coordinated PSD and MiCA frameworks, in particular through the clarification and structuring of the statuses of PSP and CASP.

In this regard, at the request of the European Commission, the European Banking Authority published an opinion in June 2025 that notably emphasised the need to comply with certain provisions of PSD2, including strong customer authentication for access to crypto-asset wallets and payment fraud reporting. The aim is to thereby ensure a high level of consumer protection, regardless of the means of payment used (EMTs or "traditional" funds). The EBA also pointed out that consumers and other market players need to be adequately protected and have a high degree of confidence in the stability of the market and the reliability of payment transactions in order to enable efficient and secure retail payments.

5.2 Challenges related to the security of the payment system

DORA (the Digital Operational Resilience Act), the European regulation on cyber resilience in the financial sector, imposes the same cybersecurity obligations on CASPs as on PSPs, as well as the implementation of tests and procedures to control and protect information systems. However, at this stage, as blockchain infrastructure is not regulated, the use of a new blockchain by a crypto-asset issuer is not subject to any governance framework and may therefore raise security issues. Any new use must therefore be brought to the attention of the authorities and crypto-asset holders in a white paper required under the MiCA Regulation and drawn up by the issuer.

⇨ In this respect, an additional best practice to be encouraged in order to make a blockchain infrastructure secure over time, is risk analysis, including an upstream audit and a regular downstream audit of blockchains, taking into account any new added features.

These resilience issues also apply to existing infrastructure. CASPs must therefore comply with MiCAR and DORA requirements and, in particular, put in place operational IT risk management policies.

5.3 Challenges related to the security of payment players and assets

Going beyond the security aspects, accepting payments using crypto-assets requires professionals – merchants or technical service providers integrated in the payment solution – to use a duly authorised third-party service provider.

⇨ The entity responsible for executing the transaction and converting crypto-assets into a legal tender currency must be approved (by the AMF if established in France) as a CASP.[31] The entity making the payment in euro to a merchant's accounts must be approved (by the ACPR if established in France) as a PSP or as a PSP agent.

Similarly, crypto-assets offered by operators must comply with the regulatory requirements. As such, merchants and their service providers must select assets before accepting them for payment and strictly refuse those that do not comply with regulations.

⇨ In this regard, several market authorities, including the AMF,[32] are calling for a strengthened European framework for crypto-asset markets (with a potential adjustment of the MiCA Regulation). They recommend that consideration be given to issues such as strengthening the rules for platforms operating outside the European Union, better supervision of platforms given cyber risks, and direct supervision by the European Securities and Markets Authority (ESMA) for significant CASPs. Their aim is to ensure that the rules for European players are applied uniformly.

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

30 The European rules on strong customer authentication are specified in a delegated act of PSD2: Regulation (EU) No 2018/389 detailing the transactions subject to these rules.

31 The issuance of electronic money tokens is restricted to credit institutions (CIs) and electronic money institutions (EMIs). The provision of crypto-asset services, the list of which is defined in Article 3 of the MiCA Regulation, is restricted to crypto-asset service providers (CASPs).

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

RECOMMENDATIONS

The Observatory would first like to stress that crypto-assets present numerous risks (associated with volatility, liquidity, default, money laundering and terrorist financing, high transaction costs, etc.), which do not fall in the strictest sense within the security issues addressed in the recommendations below. They require heightened vigilance on the part of their users and the competent authorities.

On the basis of this monitoring study, the OSMP is issuing the following recommendations on the security of payment solutions using crypto-assets in the context of everyday purchases of goods and services.

RECOMMENDATIONS FOR CONSUMERS AND MERCHANTS

Recommendation No. 1
Stay alert to attempted fraud

The Observatory recommends that users interested in payment solutions using crypto-assets verify the regulatory authorisations of the providers and the crypto-assets used. Crypto-assets that are not authorised in the European Union should be refused.

The Observatory also reiterates its general security recommendations: never respond to unsolicited approaches, never click on sponsored links (visit the website directly), never validate transactions that you did not initiate, etc.

Regulatory authorisations for crypto-asset service providers (CASPs) and for payment service providers (PSPs) can be checked on the websites of the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA), respectively. Providers who are operating illegally can also be identified through the ACPR and AMF blacklists.[33]

Recommendation No. 2
Ensure the security of sensitive payment data

The Observatory recommends that end users of payment solutions using crypto-assets protect their stored private keys, in accordance with the type (physical or digital) of wallet:

- by keeping their device in a secure location, not saving their recovery phrase online, and making sure their password is strong;[34]
- by strongly authenticating themselves on the exchange platform or non-custodial wallet provider;
- by never disclosing their sensitive payment information in the event of a request by telephone or email from a third party;
- by regularly updating devices and private key storage media to the latest, most secure versions;
- by protecting themselves against unsecured connections, such as unsecured public networks, and by using a secure internet connection and a virtual private network (VPN) to protect their data on the internet and allow them to browse anonymously.

Recommendation No. 3
Favour payments using regulated assets such as electronic money tokens

The Observatory recommends that users and merchants interested in these solutions favour crypto-assets issued by entities governed by MiCA Regulation, such as electronic money tokens, for everyday payments, in order to benefit from the security provided by the regulatory framework governing them.

Recommendation No. 4
For merchants, favour the use of dynamic QR codes

Static QR codes made available to customers pose a risk of fraud (quishing). Consequently, static QR codes for cash register systems without digital displays are less secure.

RECOMMENDATIONS FOR PARTICIPANTS IN THE CRYPTO-ASSET PAYMENT SECTOR

First, the Observatory recommends the proposals[35] **published in 2025 by the "Working Group on Smart**

Contract Certification", under the aegis of the ACPR-AMF Fintech Forum, on the auditing, governance and regulation of smart contracts.

Second, the Observatory also recommends that crypto-asset payment solution providers follow its 2023 recommendations for anticipating quantum risks (take stock of the security measures in place, test post-quantum algorithms, and draw up a roadmap for anticipating risks related to quantum computing).[36]

Recommendation No. 5
Ensure an equivalent level of protection, by regulated and unregulated players alike, by implementing strong customer authentication rules within the meaning of PSD2 for all payment solutions using crypto-assets, including non-EMT crypto-assets

Payments using crypto-assets necessitate the participation of a large number of players. By strictly following the security principles set out in the second European Payment Services Directive (PSD2), the Observatory reiterates that strongly authenticating the payment process (access to accounts or wallets, initiation of a remote payment, sensitive operations such as changing passwords, IBANs or trusted devices) is essential.

It is therefore all the more important to apply these rules to all players offering payment solutions using crypto-assets, whether regulated or not, given the assets offered (EMT and other crypto-assets) for payment transactions using crypto-backed cards or crypto-asset wallets, as well as the need to protect sensitive payment data.

Recommendation No. 6
Ensure a degree of real-time monitoring of payments using crypto-assets equivalent to that in place for traditional payments

The Observatory invites the players in the crypto-asset payment chain to ensure a degree of monitoring equivalent to that applied to traditional payments (in particular by assessing the individual risk level of each transaction) in order to effectively combat fraud.

Recommendation No. 7
Favour the use of wallets that incorporate MPC private key management techniques

Using wallets that have MPC computation technology significantly enhances the operational security of payments using crypto-assets. Having this technology integrated into a wallet therefore avoids the vulnerability associated with using traditional wallets.

Recommendation No. 8
Carry out a risk analysis before using any new blockchain and continue to monitor it over time, particularly as the blockchain evolves

In order to ensure the security of the infrastructure, the Observatory recommends that crypto-asset issuers wishing to use a new blockchain as part of their activities first carry out a risk analysis and ensure that the chain offers a high level of security. It is also important to audit the blockchain regularly, as it inevitably evolves over time as functional updates are made. Naturally, the scope of these analyses must extend to the processes external to the blockchain that aim to improve its operational performance.

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 These proposals are primarily aimed at decentralised activities, but can also apply more broadly to centralised activities.

36 Chapter 3 (pages 37-53) of the *Annual Report of the Observatory for the Security of Payment Means 2023*: "Quantum computing and the security of bankcard payment systems".

Published by
Banque de France

Managing Editor
Érick Lacourrège
Director General Cash and Retail Payments
Banque de France

Editor-in-Chief
Julien Lasalle
Deputy Director Cash and Retail Payments Policy and Oversight
Banque de France

Editorial Secretariat
Pierre Bienvenu, Clément Bourgeois, Trân Huynh, Fatih Kurt, Armand Thomas and all the members of the 2025 OSMP technology watch working group

Translator
Scott Oldale

Technical production
Studio Création
Press and Communication Directorate

Contact
Observatory for the Security of Payment Means
Internal mail code: S2B-2323
31 rue Croix-des-Petits-Champs
75049 Paris Cedex 01

Legal deposit
September 2026
ISSN 2557-1230 (online version)
ISSN 2556-4536 (printed)

Internet
www.observatoire-paiements.fr

www.banque-france.fr