DNB Payments Strategy 2022-2025

DeNederlandscheBank
EUROSYSTEEM

Content

Introduction and summary

Trends and innovations in payments are moving fast. Contactless payment by debit card, smartphone or even a watch has quickly become a standard means to pay. The same can be said of payments via QR code. New market players have emerged in the payment chain, including FinTech and BigTech companies. At the same time, a slew of new cryptos are entering the market. Central banks around the world are developing their own digital currencies to complement the declining cash-based payment methods such as banknotes and coins.

Amidst all these innovations, our task is to ensure that society can continue to rely on the payment infrastructure. Without trust, the monetary system – and the growth of prosperity – may falter. Digitalisation is a recurring theme in this new Payments Strategy. We welcome digitalisation and innovation. It makes payments more user-friendly for a large part of society, but at the same time it raises new concerns and questions. The reliable operation of the payment system must never be in question, even in a changing landscape that caters for smooth payments. This Strategy describes DNB's position and sets out the appropriate actions. It has resulted in the identification of three key priorities for the 2022-2025 period.

Key priority 1: Maintaining a robust and secure payments infrastructure

Digitalisation has greatly increased the dependence on electronic infrastructure. A failure of systems would be unthinkable. Extensive efforts must therefore be made to ensure that the millions of daily payment transactions can be processed securely at all times, including in the increasingly digital era when cybercriminal attacks may be more frequent, sophisticated and disruptive. Key focus areas are:

- **Having fall-back payment options in place for debit card payments.** With cash being used less and less, it is important that there are sufficient adequate electronic fall-back options for debit card payments. Alternative payment options must be widely available and accessible to everyone, including vulnerable groups. It is up to the market to speed up developments and to deliver, and we intend to play a driving role in this.
- **Preventing outages and combatting fraud.** In addition to regular supervision and oversight, special attack simulation tests (TIBER-NL) will be conducted to maintain resilience against cyberattacks. We will extend the tests to systemically relevant third parties on a voluntary basis. We will also actively disseminate knowledge and advice, share our TIBER-NL experiences and best practices with other vital sectors and actively engage in promoting cyber resilience in Europe. As a member of the Security Working Group of the NFPS we will continue to monitor all forms of payment fraud.
- **Maintaining the right balance between consumer protection and smooth functioning of the payment infrastructure.** There are many public interests at stake in the payments traffic, ranging from data protection, competition and financial supervision to safeguarding the smooth operation of the vital payment systems. These interests are increasingly converging. Where they overlap, the overarching public interest must be taken into account. We will therefore work with other supervisory authorities, such as the Netherlands Authority for Consumers and Markets (ACM), the Dutch Authority for the Financial Markets (AFM), the Dutch Data Protection Authority (AP) and Radiocommunications Agency Netherlands (Agentschap Telecom). In view of the changing payment landscape and overlapping issues, we are aiming for closer, more structural co-operation with these authorities.

- **Implementing European crisis coordination.** Given the international integration of the payment infrastructures, there is a need for international crisis coordination so that authorities can ensure a coordinated response to major incidents. We already have such a structure in The Netherlands. We will engage actively in international consultations with a view to establishing a European crisis coordination structure.

Key priority 2: Ensuring access to payments

Some people in vulnerable groups find it increasingly difficult to use payment services. They are experiencing a deterioration of accessibility and availability, according to the 2021 Accessibility Monitor. In some cases cash is becoming harder to obtain and use. In addition, some customer groups find it difficult to open payment accounts and access services because financial institutions exclude them in advance as part of their integrity and compliance policy ('de-risking'). Key focus areas are:

- **Paying extra attention to vulnerable groups.** Vulnerable groups are experiencing a deterioration in the accessibility and availability of payment services. The aim is to reverse this trend so that as many people as possible can continue to make payments independently. We actively support the implementation of the Action Plan for Accessible Payments, as adopted by the National Forum on the Payment System (NFPS), and want to see this Action Plan delivering positive results. We will thus fulfil one of our Corporate Social Responsibility (CSR) objectives.
- **Ensuring that cash continues to function as a means of payment.** As more and more payments are made electronically, the distribution of notes and coins is under pressure because the decrease in the cost of the cash distribution chain is not keeping pace with the decrease in cash payments. Therefore, together with the organisations involved in the National Forum on the Payment System (NFPS), we are preparing to reach agreement on the availability and acceptance of cash. These efforts should soon result in the Cash Covenant. The aim of these agreements is to ensure that people who wish to pay with cash can continue to do so despite the further rise in electronic retail payments. We will monitor and encourage the successful implementation of the Cash Covenant.
- **Involving new players in the payments market in our combined efforts to keep the payment system accessible and secure.** In the NFPS a range of stakeholder organisations from retailer and consumer associations through to payment service providers collaborate on issues relating to security, efficiency and accessibility. The natural collective responsibility for the payment system as a whole is under pressure due to the changing payment landscape and the emergence of new market players. We therefore aim to evaluate and strengthen the effectiveness of the NFPS in the period ahead and rebuild that collectivity.
- **Preventing money laundering and terrorist financing, without excluding entire categories of customers.** Money laundering and terrorist financing undermine the financial system. We expect payment service providers to assess the money laundering and terrorist financing risks posed by each individual customer and not to withhold access to bank and payment services from entire categories of customers. We ask payment service providers, stakeholder organisations and customer groups to address integrity risks, such as the risk of money laundering and terrorist financing, without unnecessarily hindering the accessibility of the cash and non-cash payment system.
- **Preparing for a digital euro so that it can be introduced if required.** It is important that public money remains accessible. The number of payments that consumers make with public money issued by a central bank, in other words cash, is declining steadily. However the convertibility of private money into public money is key in order to maintain trust in the monetary system. The ECB is therefore examining the possibility of introducing a digital euro alongside cash. We are actively participating in this study given its strategic importance.

Key priority 3: Strengthening European and global payments

The international playing field is fast-moving. Large technology companies are increasingly entering the payment chain, along with specialist FinTech companies. Banks and payment institutions have long played the main roles in the payment infrastructure, along with major international card companies. The arrival of new market players may spur greater competition and innovation, but it also entails risks with respect to privacy and with regard to market power, and dependence on non-European parties. It places a further strain on the business models of the existing parties in the chain. Harmonisation and standardisation in Europe need to pick up pace to build a stronger internal payments market. This applies also to payments to and from non-EU countries, which are still often costly, slow and inefficient. Key focus areas are:

- **Supporting pan-European initiatives which harmonise and standardise payments.** The Netherlands with its efficient, high-quality payment market, is a digital front-runner in Europe. This achievement can never be taken for granted. It needs continuous investment at a time when income for payment service providers is under pressure from the low interest rate environment and run costs are on the rise. To ensure the proper functioning of the payment system, The Netherlands stands to benefit from a more European approach. Paying easily and in the same way anywhere in Europe will benefit all EU citizens. The European payments system will become stronger if European market players can cater for this, thereby reducing dependency on American or Asian players. It will also help to better protect the sector from privacy breaches and security issues. That is why we are committed to harmonisation and standardisation, and why we support private initiatives that offer pan-European solutions.
- **Working to make cross-border payments faster, cheaper, more inclusive and more transparent.** The processing quality of these payments should be comparable to that of European payments. Meeting these objectives will require extensive cooperation between public and private sectors worldwide. We are actively participating in the plan launched by the G20, the world's twenty largest economies, and are committed to improve cross-border payments.
- **Actively contributing to the global approach to stablecoins.** Stablecoins could play a part in a faster, cheaper and more inclusive global payment system, but also pose many risks. For instance, the value of stablecoins is not as stable as the name suggests. Stablecoins must be regulated appropriately, proportionally and in line with the risks. The European Commission is currently working on regulation for cryptocurrencies, including stablecoins. The draft Markets in Crypto Assets Regulation (MiCA) includes rules for crypto issuers and crypto services providers. An important aspect of this draft regulation is supervision of stablecoin reserve management. Differences in the global regulation of stablecoins should be avoided as far as possible, because stablecoins are borderless. International coordination is required in the drafting of regulations. The Financial Stability Board (FSB) fulfils an important role in this regard, and we are actively involved. We will also issue publications on new developments relating to stablecoins, cryptos and decentralised finance.

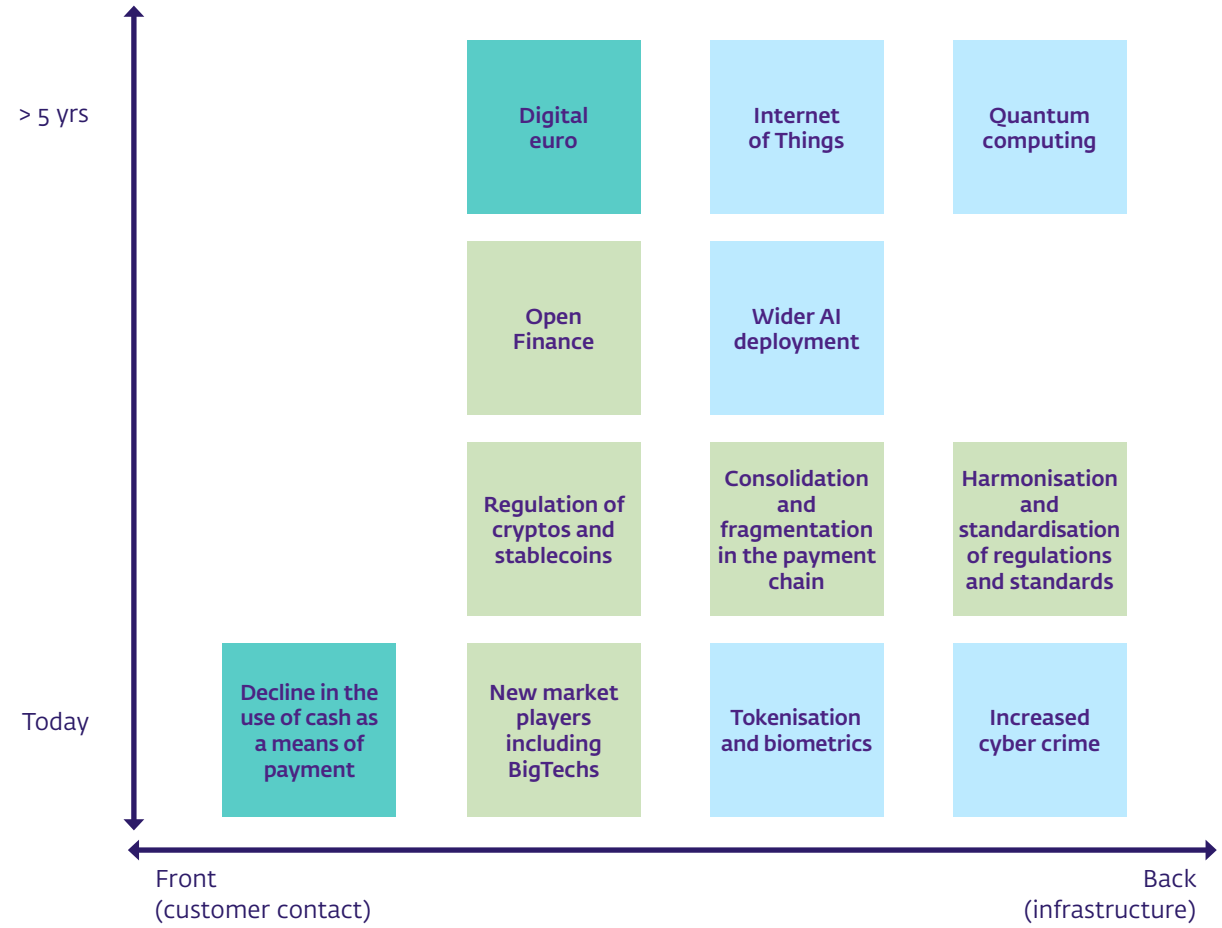
Reader's guide

This publication discusses three key priorities aimed at secure, accessible and efficient payments. The three key priorities are considered in the context of relevant trends (see the overview in the figure on the right). The key priorities are accompanied by a strategy and details of our commitment to it. Some topics, such as a digital euro, concern all key priorities. These are described in Boxes.

Key priorities

- Maintaining a robust and secure payments infrastructure in the face of greater digital dependence
- Ensuring access to payments in an increasingly digital world
- Strengthening European and global payments in a dynamic international playing field

Key developments in the payments area



Note:
This figure summarises the main developments in the payment system. It shows the approximate period and the part of the payment chain in which they will take place. The colour of the blocks indicates the key priority in which the development is described in greater detail. The figure is indicative and provided only for illustration purposes.

Key priority 1

Maintaining a robust and secure payments infrastructure in the face of greater digital dependence

Innovations and consumer and business preferences have led to the Dutch payments traffic becoming largely digital in recent years, making it more user-friendly for many people. There is a downside, however. Digitalisation and the decline in the use of cash lead to greater dependence on the digital payment infrastructure. At the same time, cyber risks are increasing and criminals are looking for new ways to commit fraud. This entails risks for the reliable operation of the payment system. The need to guarantee robustness and security will therefore become even greater in the years ahead. In order to maintain robustness, our focus in the next few years will be on the adequate availability of electronic fall-back options in the event of an outage in the electronic payment system. We also advocate the creation of a European crisis coordination structure. We are strongly committed to cyber resilience and fraud prevention to guarantee security.

Trends and developments

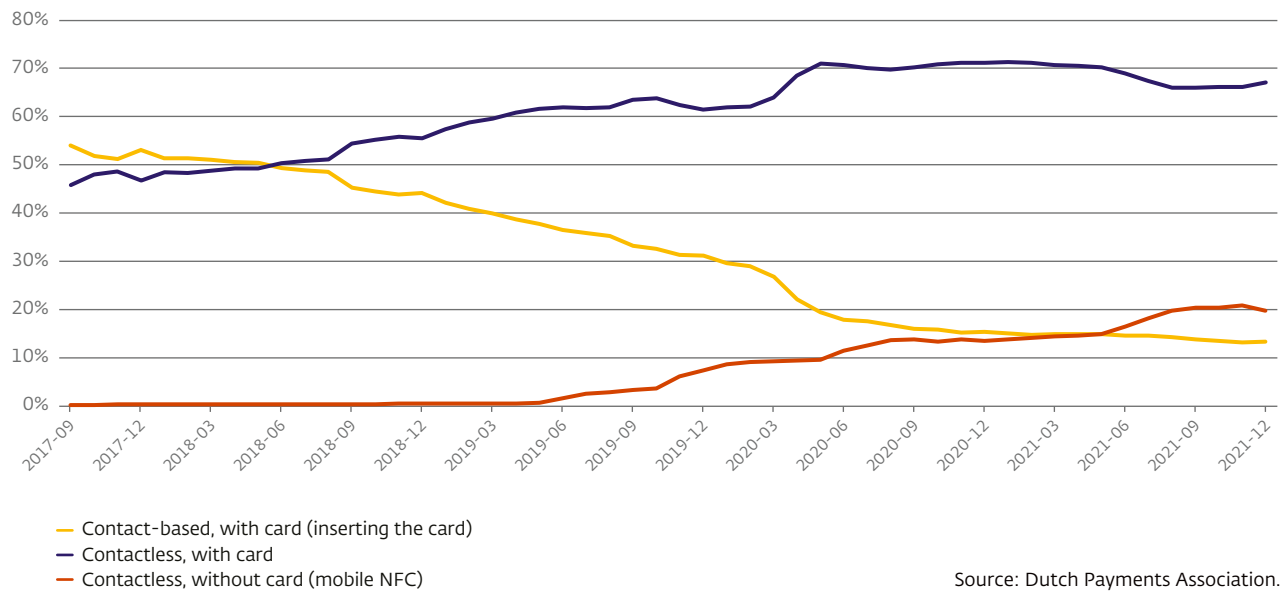
The coronavirus crisis has given renewed impetus to the digitalisation of payments. The use of cash at points of sale is falling steadily and we are increasingly using digital payment methods. In 2015 for the first time more point-of-sale payments were made by debit card than by cash. By 2019 almost 70% of payments were made by debit card, compared to 30% by cash. The coronavirus crisis has further accelerated the digitalisation, which has also been encouraged by DNB and the financial sector. Only two out of ten payments are now made by cash. Consumers have also made greater use of contactless payments since the coronavirus crisis. Following the introduction of Apple Pay in the Netherlands in June 2019 the number of contactless payments made by mobile phone has also risen steadily (see Figure 1). This rise is expected to continue, spurred by new providers, as recently in the case of Google Pay. Consumers have increased their online purchases during the coronavirus crisis, so the number of online payments has also increased substantially. This is expected to be a lasting trend. Consumers have become used to digital payment methods and also trust them, according to our research.[1]

Modern technologies are opening the way to new payment methods. Mobile payment has been made possible by tokenisation, for example. This technology replaces data, such as credit or debit card information, with a unique combination of letters and/or numbers known as a token. Tokenisation enables a digital version of a debit or credit card to be stored in a digital wallet. This technology forms the basis for contactless payment using a smartphone or other wearables, such as a smartwatch. It also makes payments more secure, because not all data has to be transmitted along the entire chain. QR code payments have also rapidly gained in popularity. QR codes are used in the hospitality industry and by several charity organisations, for example.

1 See for example Bijlsma, M., C. van der Cruijsen, J. Koldijk (2021), Determinants of trust in banks' payment services during COVID: an exploration using daily data, DNB Working Paper 720; Bijlsma, M., C. van der Cruijsen, N. Jonker and J. Reijerink (2021) What triggers consumer adoption of CBDC?, DNB Working Paper 709, or the DNBulletin Safe payments are fundamental to sustaining trust and confidence in the payment system.

Figure 1 Contactless payments by card or mobile phone is gaining ground in the Netherlands

Percentage of debit card payments



Source: Dutch Payments Association.

In the future more payments could take place by means of the Internet of Things (IoT). IoT enables devices to communicate with each other via internet connections. Specific uses of IoT include refrigerators, cars and other products that carry out payment transactions on behalf of (and with the explicit approval of) the consumer. Examples include a coffee machine that recognises when it is running out of coffee beans and orders more and a car that automatically pays highway tolls so the driver does not have to stop. Supermarkets are also experimenting with new technologies that record the contents of a shopping basket so payment no longer has to be made at the checkout or self-scan terminal. Customers can leave the store immediately with their groceries, and the payment is taken automatically. This provides greater convenience for the consumer and offers improved throughput and efficiency for the retailer. Artificial intelligence and 5G are likely to boost new payment solutions, for example those using IoT, but these technologies also bring their own complications. In the more distant future quantum computing (using quantum computers with very high computing power) may also have an impact, including with regard to the security of the payment system, although it will be some years before the potential applications become clear.

> "Innovations make payments more user-friendly for many users."

Payments are increasingly frictionless, which makes them more user-friendly, but there is also a downside. Digital transactions are increasingly verified by means of biometrics, for example. Biometrics concerns the use of physical characteristics, such as iris scans, facial recognition and fingerprints, for identification, authentication and authorisation purposes. Two-factor authentication has been mandatory since the introduction of PSD2 (Payment Services Directive 2), the revised European payments directive. The factors must be two of the following three: something that you are (biometrics), something that you have (device) and something that you know (PIN). Biometric applications are evolving rapidly and use new techniques to optimise the digital access control process. This helps to ensure that the payment process is as simple as possible. There is a downside, however. Frictionless payment can detract from the sense of control and security if there is so little friction that a person has already paid before they realise it. It can also make budget management more difficult,

increasing the chance that some people will get into financial difficulty. The same applies in the case of buy-now-pay-later (BNPL) options, which are increasingly common in the payment system. BNPL enables consumers to buy a product and to pay all or part of the price later. This links lending and payment.

Innovations in the underlying infrastructure allow faster payment and settlement. As well as consumer payment technologies, there is also an underlying corporate infrastructure. At the centre of this is TARGET2, the payment system of the ECB and other central banks in the euro area. This system is used by banks and financial market infrastructures. The institutions that process electronic payment transactions, for example, also settle their payments through TARGET2 at the end of the day. This system is due to be overhauled in the coming year and will be merged with TARGET2-Securities, which facilitates the settlement of securities transactions. These are transfers of shares and bonds for the business market. The consolidation of the two systems should make payments between member institutions easier, more efficient and more secure. Other possible innovations in the underlying infrastructure are the accelerated processing of securities and longer opening hours for the new Target Services platform.

Financial institutions and financial market infrastructures are experimenting with Distributed Ledger Technology (DLT), which enables them to operate on a decentralised basis. DLT could increase the efficiency of the settlement process, as it would speed up communication between various market players and make reconciliation and intermediaries redundant. There are nevertheless outstanding issues to resolve with regard to governance, risks and real-time oversight of systems using DLT and interoperability with existing financial systems. Unlike traditional financial institutions and financial market infrastructures, DLT systems can exist without a centrally accountable and responsible organisation. The question is then who is responsible for (among other things) implementing an appropriate integrity policy, including anti-money laundering (AML) policy.[2] DLT has shown its potential in recent years and is set to become part of the market infrastructure, so there is a more urgent need to draw up clear rules on the governance of these systems and the organisation of oversight. This will therefore be an important focal point over the next few years and will require international cooperation within the Bank of International Settlements (BIS) and the Financial Stability Board (FSB), as this type of infrastructure can easily operate internationally. The basic principle is: "same business, same risks, same rules".

Advancing digitalisation will lead to greater dependence on the existing digital payment infrastructure. The Dutch point-of-sale (retail) payment system has long been heavily dependent on the digital and card payment infrastructure. This entails risks for the smooth operation of the payment system. Adequate fall-back options must be available if the infrastructure or card system fails. Cash only provides a partial fall-back option. Therefore, alternative digital payment solutions are needed that are easily accessible to all Dutch citizens, including the more vulnerable groups. The introduction of instant payments in 2019 has provided an alternative non-cash infrastructure that has such potential. Currently, however, instant payments are mainly used for fast transfers and only to a limited extent for payments in store or at the door. Alternative payment methods (such as iDEAL QR codes and offline debit card payments) are already or will become available, but they will not provide a fully-fledged alternative until they have been rolled out widely.

The increased digitalisation and growing complexity of the payment chain may also have consequences for the robustness of the payment chain. A growing number of players are becoming involved in the payments chain (see also key priority 3). Financial

2 Traditional financial institutions that plan to use DLT are of course already subject to regular supervision, so in those cases it is clear which party will bear responsibility for compliance with AML rules.

institutions increasingly use third parties for ICT systems, cloud services, data and software. This increases efficiency and cuts costs. But the combination of greater dependence on external service providers and a more complex payment chain with new, innovative parties also entails risks. These are outsourcing risks, including concentration risks because financial institutions often source services from the same operator. This applies, for example, in the case of cloud services. The greater complexity also makes it more difficult to see all the dependencies in the payment or securities chain and to respond appropriately to technical outages or cyberattacks.

The forthcoming Digital Operational Resilience Act (DORA) provides a harmonised European regulatory framework to respond appropriately to the trend of increasing digitalisation in the financial sector and the attendant risks. DORA will cover not only risks relating to the operational security, stability and continuity of financial institutions, but also the fact that financial institutions are increasingly outsourcing activities to a relatively small circle of ICT service providers. The Act will introduce oversight[3] of critical, international technical service providers such as cloud companies. Since DORA will apply to a wide range of institutions, it will play an important role in supervision.

> "Our dependence on the digital payment infrastructure is growing, while cyberattacks are increasing"

Cyberattacks are on the rise and have an increasingly disruptive impact. A protracted outage or failure of cash and electronic payments in stores, remote payments, commercial payments or securities transactions could cause serious social disruption and economic damage. Cyber resilience is therefore immensely important, particularly as cyberattacks are on the rise. The number of ransomware attacks, for example, has risen sharply since the start of the coronavirus crisis.[4] Institutions in the financial sector and/or third parties in the same value chain are also regularly affected.[5] There is also the constant threat of DDoS (distributed-denial-of-service) attacks, in which the perpetrator attempts to render an online service inaccessible. Although Dutch financial institutions have taken extensive measures to counter such attacks in recent years, ensuring that the continuity of the payment and securities systems has never really been in question, this threat remains very real. The trend towards outsourcing of vital processes (including payments) makes financial institutions more vulnerable to disruptions of their service providers' operations. Third parties such as ICT service providers specialise in what they do and generally set great store by security, but they are also regular targets of digital attacks, partly because third parties can be used as a springboard to gain access to multiple customers.

Payment fraud is focused increasingly on humans as the weakest link in the system. Traditional fraud such as skimming is no longer lucrative due to the measures that have been taken (such as the use of EMV chips and strong customer authentication), so criminals are devising new ways to commit fraud. They are using social engineering, i.e. abusing people's trust, ignorance, fear, curiosity or greed to extract confidential data from them. Fraudsters use sophisticated methods. For example, they first try a fake request for help and then (posing as the bank) call the target to 'warn' them. The target then falls victim to bank helpdesk fraud. Many people are affected by such scams. Losses due to fake requests for help, for example where someone requests money by WhatsApp, and bank helpdesk scams (telephone spoofing) are rising sharply. Losses from bank helpdesk scams reached around €40 million in 2021,

3 Oversight is the supervision of parties that are active in the payment and securities industry, such as settlement agents, central counterparties and securities depositories. A licensing system is in place and the means of enforcement under the Financial Supervision Act are also applicable.
4 Cyber Security Assessment Netherlands 2021.
5 See also the Information Security Monitor 2021.

a rise of almost 50% compared to 2020.[6] With this type of fraud it is the customer who transfers the money, so banks do not in principle refund the loss. Following a public debate the banks decided in December 2020 to take a lenient stance and to compensate customers for losses due to bank helpdesk fraud combined with telephone spoofing, retroactively from the start of 2020, in cases where the name or telephone number of the victim's bank were demonstrably abused and the victim reported it to the police.

Strategy

We support innovations and technological developments in the payment system and keep a close eye on any new risks. We are committed to facilitating innovations in the market as effectively as possible. For example, firms can exchange views with us and other supervisory authorities in the annual Fintech meets the Regulators seminar. We welcome legislative initiatives such as the European DLT Pilot Regime, which allows market infrastructures to apply DLT under certain conditions. This initiative is an important step towards creating the right framework for more experimentation with innovative technologies. We are launching experiments with DLT applications jointly with the sector. The primary aim is to increase knowledge in preparation for tackling issues that flow from these DLT applications in relation to supervision, financial stability and monetary policy. Together with the sector we also want to make sure the Dutch financial infrastructure is well prepared for possible changes in payment and securities systems. We also support research into possible additions to the TARGET2 services, in which the Eurosystem provides central bank money that can be used for DLT applications in the interbank payment system or deploys other solutions that facilitate blockchain transactions with central bank money. We will also examine whether it is possible to expand access to our own systems, for example for new and innovative payment service providers, in a secure manner. If innovations in the payment system lead to undesirable risks, we will take action. For example, we will engage in discussions with relevant parties, consult the National Forum on the Payment System or take additional measures as part of our oversight.

We are committed to the creation of adequate electronic fall-back options for debit card payments. The reliability of the debit card payment system is high (99.89% in 2020), but it will never be error-free and there will always be a risk of a major cyberattack succeeding. Now that cash is being used less and less, we need sufficient digital alternatives to the debit card systems, which must not fail for the same reason as debit card payments. They must also be widely available and readily usable by all consumers, including those who have difficulty with digital means of payment, in the event of an outage in the electronic payment system. It is up to the market to speed up developments, and we intend to play a driving role in this. We believe it is particularly important to maintain a degree of diversity in payment solutions to increase the robustness and accessibility of the payment system. The instant payments infrastructure has the potential to be one of the viable alternatives, as long as it can be accessed by a suitable method such as QR codes. Offline debit card payments also offer opportunities. If the European Central Bank issues a digital euro in the future, it could also serve as a fall-back option for debit card payments (see also Box 3).

6 These are provisional figures for 2021; the final figures were not yet available at the time the Strategy was published.

We will continue to focus on cyber resilience in the years ahead. We will work with the sector to obtain the most up-to-date picture of cyber threats, In addition to the regular supervision, special attack simulation tests will be conducted to maintain resilience against cyberattacks (TIBER-NL: threat intelligence-based ethical red teaming).[7] These tests show generally high levels of cyber resilience. At the same time they show that sophisticated attackers could potentially cause a lot of damage to institutions that are essential for financial stability. There is a real probability that attackers will ultimately succeed in penetrating a financial institution. Therefore it is not sufficient to focus solely on the prevention of cyberattacks. Close monitoring, rapid detection and appropriate crisis response are also crucial.[8] We will also actively disseminate knowledge and advice. We are already doing so, for example through the Information Security Monitor. A new feature is that we will also use other forms of communication, including white papers on current threats. Finally we will examine the challenges and opportunities facing the sector in the field of cyber resilience, share our TIBER-NL experience and best practices with other vital sectors and stay actively involved in promoting cyber resilience in Europe. After all, hackers do not operate solely within national boundaries.

As a member of the Security Working Group of the NFPS we will continue to monitor all forms of payment fraud. Banks, the police and the Public Prosecution Service, but also, for example, BigTechs and telecom operators are working closely together on this matter. An integrated approach is essential to combat fraud effectively. Public information also remains a very important means of raising awareness of social engineering fraud.

We underline the importance of a European crisis coordination structure. Payment and securities processes are vitally important. A crisis management structure has been established at national level to deal with any operational disruptions to these vital processes. DNB, AFM and the Ministry of Finance work with financial institutions within this structure. They exchange information and take action in the event of actual or threatened serious operational disruptions with potentially serious social and/or financial consequences, regardless of the cause. There is also a need for a crisis management structure at European level, with alignment between national structures. This must be established in the next few years. In parallel with the new DORA legislation, work is already under way to establish a pan-European coordination structure for cyber incidents. This structure should enhance the ability of authorities to provide a coordinated response to potential major cyber incidents.

We highlight the importance of robustness of financial market infrastructures (FMIs) that handle securities and derivatives transactions. These include central counterparties (CCPs) and central securities depositories (CSDs), for example. The objective here too will be to have institutions that are solid and able to manage their risks. For example, various long-term programmes have been established, partly at our request, to strengthen the cyber resilience of this post-trade sector. But robustness also means that these institutions pose no threat to wider financial stability in the Netherlands and that they are able to handle securities and derivatives transactions in a secure and appropriate manner. This also means we will continue to look critically at the extent to which Dutch parties retain access to CSD services. At the same time we will analyse the impact of any market changes on the market positions and our oversight of the institutions concerned.

7 The institutions participating in the TIBER-NL programme hire specialist firms to carry out controlled attacks on financial institutions' critical systems based on the most up-to-date threat information. Experts from the financial sector, the intelligence services, the police and the National Cybersecurity Centre work together to ensure the availability of up-to-date information on cyberthreats.

8 See the Autumn 2020 DNB Financial Stability Report, Cyber risks in the coronavirus era

In view of Brexit and the resulting changes in the playing field we will devote particular attention to the continuity of the services provided by central counterparties (CCPs). Securities and derivatives transactions are increasingly settled through a central counterparty (CCP) to increase the stability and transparency of the financial system. A CCP is positioned between parties to a derivatives contract or securities trade and assumes their liabilities in order to reduce their counterparty risks. As a guarantee, the CCP requests collateral from the trading parties. Multilateral netting also reduces the total outstanding position in the market, which generally improves efficiency and security. Central counterparties settle transactions on the basis of "delivery versus payment" (the acquirer gains legal possession of the security when payment has taken place). For that purpose CCPs' clearing and settlement activities are linked to the Eurosystem's payment systems (TARGET2 and TARGET2-Securities). A large proportion of the clearing of euro-denominated interest rate and credit derivatives currently takes place through CCPs based in the United Kingdom. Brexit is changing the context in which these CCPs operate. European players can still use UK CCPs to clear interest rate and credit derivatives. That is beneficial for continuity of service, so we opposed any prohibition of such access. This market nevertheless appears to be shifting slowly to the European mainland with the rapid development of financial centres in Amsterdam and elsewhere. Against this background we will closely monitor the availability of clearing services for Dutch financial institutions, such as pension funds, in the years ahead.

To further promote the robustness of the financial system, we will critically assess the role played by CCPs in times of market stress. The current regulations require financial institutions to build up additional buffers with the CCP at times of crisis. Margin calls are then made, whereby money is lodged as collateral in the event that a party defaults with unpaid liabilities. However, these margin calls are often made at times when liquidity is under the greatest pressure, giving rise to a procyclical effect. In international forums such as the Financial Stability Board (FSB) we will call for such procyclicality to be reduced as far as possible, for example by adjusting the models that CCPs use to calculate margins.

In view of the changed payment landscape we aim to co-operate more closely with other authorities, such as the ACM, AFM, Dutch DPA and Radiocommunications Agency Netherlands. The mandates of the various authorities in areas such as cybersecurity, data protection, competition, financial supervision and the smooth operation of the payment system are increasingly converging. Where they overlap, the overarching public interest must be taken into account, for example an efficient payment system, privacy versus data sharing from the perspective of fraud prevention and the fight against money laundering. We already collaborate with various authorities with regard to PSD2. We want to put this collaboration on a more structured footing.

Key priority 2
Ensuring access to payments in an increasingly digital world

Actions such as opening a payment account, activating a debit card, transferring money or making a payment in a physical or online store are increasingly being performed digitally. Research shows that some people in relatively vulnerable groups – such as the elderly, people with low literacy skills and people with disabilities – find this digitalisation increasingly difficult. We will make a particular effort to keep payments and payment services accessible for everyone in the years ahead. We will thus fulfil one of the elements of our own policy with regard to Corporate Social Responsibility (CSR). We are also committed to ensuring that the cash infrastructure, which is under pressure due to the declining use of cash, continues to function properly. We also want to ensure that payment service providers implement their integrity, anti-money laundering and anti-terrorist financing policies in such a way that customers are not unfairly prevented from opening a payment account, forced to close their account or restricted in their use of cash. A consequence of the reduced use of cash is that the number of payments people are making with public money issued by a central bank is declining steadily. We believe it is important that public money remains accessible because the convertibility of private money (bank deposits) into public money is essential to maintain trust in the monetary system. In the years ahead we will therefore examine at ECB level whether and how a digital euro should be introduced to supplement cash.

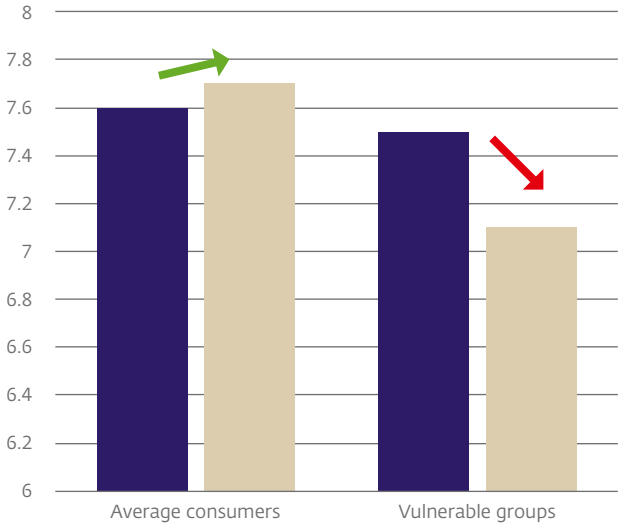
Trends and developments

The large-scale digitalisation of the payment system appears to threaten the accessibility of payment services for people who have difficulty using digital payment methods. The 2021 Availability Monitor shows that most consumers have a positive view of the accessibility of payment services and are more satisfied than they were a few years ago, but people in various vulnerable groups believe accessibility has deteriorated and thus give it a significantly lower rating on average (see Figure 2). This applies to the elderly, people with a disability (e.g. people who are blind or partially sighted, deaf or hard of hearing, wheelchair users), people with limited digital skills or low literacy, low-skilled people and those with no internet access. There is a risk that the advancing digitalisation of the payment system will open up a divide in society.

> "Digitalisation threatens some people's access to the payment system"

The accessibility of payment services for some businesses and consumers has come under pressure. Banks and other payment service providers have a statutory gatekeeper role that requires them to carry out proper assessments of the integrity risks posed by individual customers and their transactions, such as the risks of money laundering and terrorist financing. They sometimes decide to withdraw or restrict access to payment services for individual customers or a specific category of customers, or to refuse or terminate certain cash or non-cash transactions, because they associate these customers with a higher risk of terrorist financing or money laundering. This is known as de-risking. If payment service providers categorically restrict the payment services they provide to entire customer groups in advance, they risk refusing to provide payment services to individual customers without assessing the

Figure 2 Ratings for overall satisfaction with banking and payment services



Source: Availability Monitor 2021, National Forum on the Payment System.

risks associated with those customers and the how to manage them. This is undesirable in terms of the proper functioning of the payment system, because it may lead to customers who are not involved in money laundering or terrorist financing being denied access to payment services. This is not the same as wholesale exclusion for commercial reasons, for example, or due to broad CSR objectives such as the exclusion of customers that use production methods involving animal cruelty, if, in the opinion of the institution, the pursuit of sustainability through customer involvement is not feasible. In that case it is important to assess whether the market is still providing sufficient access to payment services for prospective customers who are refused access for commercial or CSR reasons.

The cash infrastructure is under pressure due to the reduced use of cash. For example, the number of ATMs and deposit facilities has declined in recent years (see Table 1), with explosive attacks also leading to the temporary closure of a large number of deposit facilities. There are also shops that no longer accept cash payments. The declining use of cash (see Figure 3) makes it relatively less attractive for commercial parties to offer cash services. That in turn makes the infrastructure vulnerable. There is a risk that the decline of the cash infrastructure will make it increasingly difficult for cash-dependent people to participate in the payment system. This would be an unwelcome development.

Another effect of the reduced use of cash is the steady fall in the number of payments made with public money. Cash has an important function as a means of converting private euros into the same amount of public euros. The convertibility of private money into public money helps to maintain trust in the monetary system. If people find it difficult to access cash when they need it, their trust in the monetary system could be be undermined. The introduction of a digital euro may provide a solution (see Box 3).

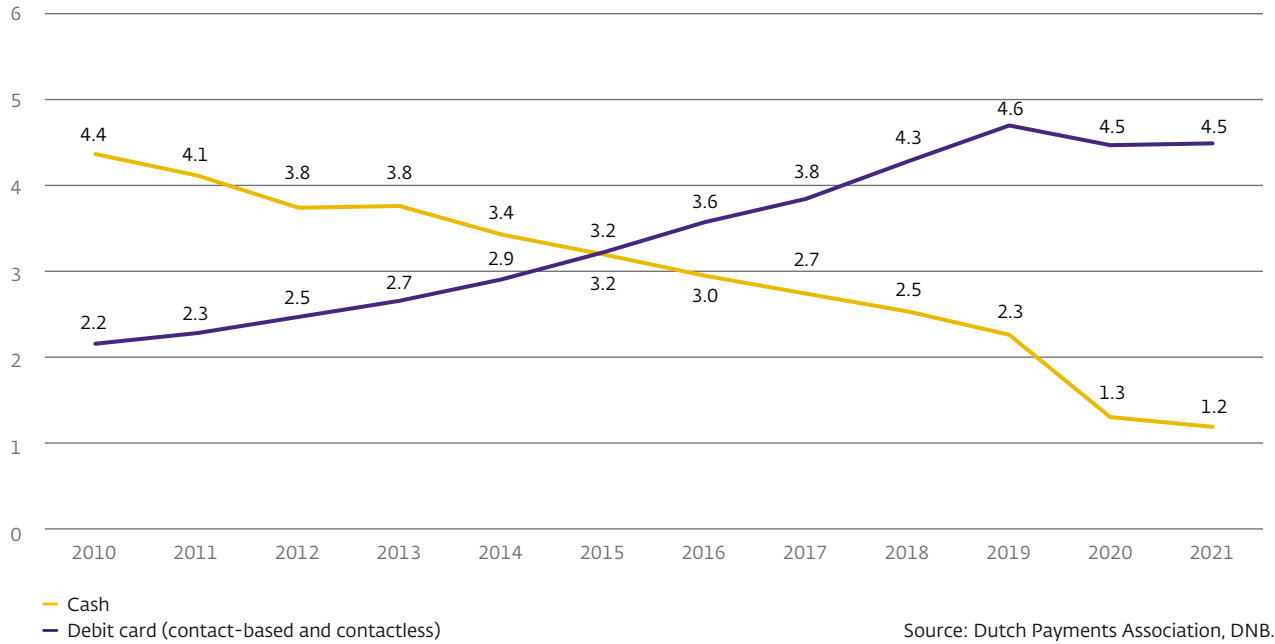
Table 1 Number of banking services 2010-2021

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Number of bank branches[1]	2,864	2,653	2,466	2,165	1,854	1,764	1,674	1,616	1,489	1,260	942	726
ATMs[2]	8,356	9,012	8,795	8,633	8,811	8,319	8,066	7,847	7,113	6,424	5,795	4,916
Cash deposit machines[3]	2,297	2,264	2,172	2,294	1,790	1,776	1,795	1,795	1,730	2,872	2,074	1,745

1 The following definition applies to bank branches: The number of branches (buildings of an individual PSP, where at least cash withdrawals and/or deposits can be made, and where payment orders can be issued or made.
2 This number includes both bank and non-bank ATMs and other cash dispensing points.
3 Cash deposit machines can be subdivided into regular cash deposit machines and seal bag machines. For 2010 to 2018, only figures for regular deposit machines are presented. For 2019 and 2020, figures for seal bag machines are also available. The majority of cash deposit machines are recyclers, which are also counted in the number of ATMs.

Figure 3 Cash payments decrease, debit card payments increase

Number of payments (in billions)



Source: Dutch Payments Association, DNB.

Strategy

We want to reverse the trend whereby vulnerable groups are experiencing a deterioration in the accessibility and availability of payment services. The aim is to ensure that as many people as possible can continue to make payments independently. This includes specific actions such as opening a payment account, receiving and activating a debit card, withdrawing and depositing cash, checking debits, credits and account balances and issuing payment orders (basic payment services). With digital payments now in the majority, we will make a particular effort – including at EU level (for example in the case of a digital euro) – to guarantee accessibility for people who, for various reasons, find it difficult to use digital means of payment. This will fulfil one of the elements of our CSR policy (see Box 1). We aim to guarantee accessibility without impeding the further digitalisation of the payment system. Financial inclusion can be achieved in two ways: by providing digital payment skills for people who need them. If that is not possible, by creating alternative physical services or providing personal support: on site in the customer's neighbourhood, on paper or by telephone. Such alternative accessible services must include an easy means to ask questions about basic payment services. Steps must be taken to ensure that these people are not merely sent from pillar to post.

> "Everyone must be able to continue to take part independently in the payment system"

Box 1 CSR in the payment system

Corporate social responsibility (CSR) is an integral part of our mission. This is why, as a central bank, supervisor and resolution authority, we are committed to safeguarding financial stability, thus contributing to sustainable prosperity in the Netherlands. We focus on two themes: 1) sustainable economic growth without harmful effects on the environment, and 2) an inclusive financial and economic system. This also relates to our work in payment and securities systems.

Sustainable economic growth without harmful effects on the environment

Reducing the carbon footprint
We aim to reduce the environmental impact of money in line with international targets such as the Paris Climate Agreement. We are updating the carbon footprint of cash and electronic payments and drawing up an action plan to reduce it. Our aim in any event is to halve carbon emissions from the cash chain by 2030 compared to 2019. The new DNB Cash Centre in Zeist is climate-neutral and thus contributes to this objective.

Assessing climate and environmental risks
We believe it is important that financial market infrastructures take account of climate and environmental risks in their risk management. They are not doing so sufficiently at present, because the current regulations on financial market infrastructures do not specifically describe these risks. We will therefore work with other operators in the Dutch market infrastructure to develop *good practices* for climate risk management. We also aim to raise awareness of these good practices internationally and will promote them in international bodies such as the Committee on Payments and Market Infrastructures (CPMI) of the BIS and the Central Banks and Supervisors Network for Greening the Financial System (NGFS).

An inclusive financial and economic system
Sustainable prosperity calls for an inclusive economic and financial system, in which financial services are readily accessible and the continuity of critical financial functions is safeguarded. We are thus committed to keeping the payment system accessible for everyone. How we will do so is explained in key priority 2 of this Strategy.

"We will reduce the carbon footprint of money in the years ahead"

The main tool for guaranteeing this inclusivity is the Action Plan for Accessible Payments agreed by the NFPS in 2021. The Action Plan aims to improve banks' personal services (at local level) for people who need support with changes in payment systems, such as those in relatively vulnerable groups. Banks will also be able to communicate better with these people about the solutions they have adopted and better assess the areas where customers need specific help. The Action Plan will be evaluated in 2023. We believe it is important that the Action Plan delivers positive results as quickly as possible and we will support and closely monitor progress.

> "Services for vulnerable people must be improved and represent an opportunity for market participants to provide added value"

We are also monitoring developments with regard to the application of the Directive on the accessibility requirements for products and services (EU 2019/882). This directive requires payment service providers to implement the UN Convention on the Rights of Persons with Disabilities and aims to make all products and services accessible to persons with disabilities. The directive is due to come into force for financial service providers by 2025 and includes provisions on accessibility for people with disabilities to facilities such as ATMs and bank branches. The government's legislative proposal for implementing the directive was submitted for public consultation at the end of 2021. We will ensure that due regard is paid to the aspects concerning the payment system. We also call on innovative parties to use their capacity for innovation and the design of user-friendly products to improve accessibility for people who have difficulty using digital payment methods.

In line with our social role, we aim to provide support and education to safeguard the accessibility and security of the payment system. Given the ongoing digitalisation of the payment system, it is important to support people who have difficulty keeping up with digitalisation. This is primarily a role for payment service providers. Here too we will contribute by providing information on the operation of various payment products, the associated risks and how we can address those risks together as effectively as possible.

In 2022 we will examine more closely the size and nature of the various groups of people who have difficulty accessing payment services. Our aim is to obtain a clear picture of these groups. It is not only the size but also the nature of the accessibility issues that matters. Moreover, the groups concerned include both people who are cash-dependent and people who are experiencing difficulty with the digitalisation of various payment services. By focusing more clearly on the problems faced by these groups it will be possible to take a more targeted approach in the existing Action Plan for Accessible Payments of the National Forum on the Payment System (NFPS).

We aim to strengthen the effectiveness of the NFPS, which among other things discusses a wide range of accessibility issues. The NFPS provides a forum in which various parties on the demand and supply sides of the payment market (banks on the one hand and senior citizens' organisations, disability organisations, the Dutch consumers' association, SME organisations etc. on the other hand) can come together under our aegis to discuss barriers to accessibility, security and efficiency and to seek joint solutions. The sense of shared responsibility for the Dutch payment system is coming under pressure due to the changing payment landscape and the emergence of new market players. We therefore aim to evaluate and strengthen the effectiveness of the NFPS in the period ahead.
An evaluation may give rise to questions such as:
are the right parties still represented in the forum?
How can we guarantee the effectiveness of the consultations in the future?

As part of their policy to limit integrity risks, we expect payment service providers to assess the integrity risks posed by each individual customer and not to withhold access to bank and payment services from entire groups of customers without conducting any individual risk assessment. We expect payment service providers to make efforts to prevent unwanted effects of de-risking. At the same time customers must also make an effort to reduce their risk profile and cooperate with objectives such as proper customer identification, verification and transaction monitoring. We want payment service providers, as well as stakeholder organisations and customer groups, to address integrity risks – individually and where possible jointly – without jeopardising the smooth operation of the payment system. Consumers have a statutorily enshrined right to open a payment account under certain conditions, but of course businesses too cannot operate without a payment account. We will maintain our dialogue on the problem areas with the sector, public authorities and customer groups in order to achieve a balance between protecting the financial sector against integrity violations and ensuring sufficient, inclusive provision of payment services, including adequate cash services. As a member of various EU bodies we will also endeavour to strike the right balance between curbing integrity risks and maintaining the smooth operation of the payment system. Some payment service providers restrict access to payment services for entire categories of customers for commercial reasons or to meet wider CSR objectives. We will monitor whether access to payment services remains adequate from that perspective.

> "Money laundering risks must be assessed on a customer-by-customer basis"

We are committed to the successful implementation of the forthcoming Cash Covenant. This Covenant is expected to be concluded soon between banks, cash service providers, consumer representatives, retailer representatives and DNB. Its purpose is to ensure that cash continues to function effectively as a means of payment, even if payments are increasingly made electronically. After all, cash fulfils several important functions in society and in the financial system (see Box 2).

> "The proper functioning of cash must be safeguarded particularly at a time of increasing digitalisation"

Given the importance of the accessibility of public money – at a time of declining cash use – the ECB is studying the possibility of a digital euro. We are actively participating in this study. Box 3 contains more information on this topic.

> "The digital euro should ensure that public money remains accessible"

Box 2 Cash Covenant

Cash fulfils various roles. Firstly, it is still an important means of payment: one in five point-of-sale payments are made in cash. There can be various reasons why people use cash. They may lack or be unable to learn digital skills. They may also want to keep a close eye on their spending or have privacy concerns. They may also be people who habitually prefer to pay with cash. Secondly, cash still serves as a fall-back option in the event of an outage in the digital or card infrastructure. Suitable alternatives are being studied, but an adequate cash infrastructure will need to be maintained until such time as these are widely available in the market. Thirdly, cash is still the only form of public money. Cash is the most secure form of money available because it is issued directly by the central bank. Cash enables private euros, such as bank deposits, to be converted into the same amount of public euros, which helps to maintain trust in the monetary system.

We are preparing to reach agreement with stakeholders to safeguard these objectives as the use of cash declines. These efforts should soon result in the Cash Covenant.

Box 3 A digital euro

The ECB is investigating the possibility of issuing a digital euro alongside euro banknotes and coins. We are actively participating in this study. A digital euro is a digital form of cash, issued by the central bank, which can be used to make payments throughout the euro area.

Why a digital euro?
We believe it is important that consumers have access not only to private money, such as bank deposits, but also to public money, such as banknotes. Private money contributes to innovation in the payment system, while the convertibility of private money into public money is important for trust in the monetary system. Private and public payment systems thus complement each other and can operate well alongside each other. Together they can strengthen the continuity and accessibility of the Dutch payment system.

With people increasingly using digital payment methods, by bank debit card or mobile phone, the use of cash is declining and hence so too is the use of public money. In the meantime we are also seeing the emergence of cryptos and stablecoins issued by private parties. Although their use in the payment system is limited at present, stablecoins in particular – if well regulated – could become a more commonly used payment method in the future. These developments will shift the balance between public and private money increasingly in favour of private money. The central bank's remit is to safeguard financial stability and an efficient, reliable and inclusive (public) payment system. A digital euro can contribute to this and ensure that euro area citizens retain access to a secure, efficient and reliable public means of payment.

Depending on its design, a digital euro could also serve as a back-up for payments in private money. Consumers and businesses could then use a reliable, stable and risk-free means of payment in any situation. This argument is gaining impetus as the risk of digital disruption becomes increasingly prominent (see also key priority 1).

A digital euro will not replace the current payment system and parties within it, such as banks and other payment service providers. A digital euro will exist alongside cash and not replace it. A digital euro will supplement existing payment products and thus contribute to diversity. We believe it is important that a digital euro is accessible to everyone, young or old, with or without disabilities. In line with our sustainable finance strategy we will actively promote financial inclusion (see key priority 2). Privacy and security must also be firmly embedded. Another precondition is the maintenance of financial stability and monetary policy transmission. Partly for that reason a digital euro will be implemented in cooperation with banks and other payment service providers.

Finally, global interoperability will be pursued to ensure that the digital euro contributes to greater efficiency in cross-border payments (see key priority 3). This could also reduce the dependence on non-European market participants – existing bank and credit card companies and new players such as BigTechs.

The ECB's Digital Euro project
In October 2021 the ECB launched the official investigation phase, which is due to run until the end of 2023. This phase will include a study of the potential uses that a digital euro must offer in order to become a risk-free, accessible and efficient form of digital public money. In the investigation phase the ECB project will focus on a possible functional design that meets users' needs. It will look at the payment options the digital euro should offer, how the digital euro can be made available and what the business

model could be. This phase also includes determining how the design and implementation rules of the digital euro can prevent financial stability risks and safeguard the privacy of users. A decision on whether to introduce a digital euro will be taken at the end of 2023, after which an implementation phase could begin.

We are actively participating in the ECB project. We are represented in various bodies in the project, including the High-Level Task Force on Central Bank Digital Currency (HLTF-CBDC), which is responsible for the project. We will also maintain an active dialogue with the relevant national stakeholders, such as market participants, the Ministry of Finance, the House of Representatives and members of the National Forum on the Payment System, to keep them fully informed and consult them on developments surrounding this project.

Wholesale digital euro

In parallel, the Eurosystem is working on a strategy for the development of solutions to facilitate future interbank payment transactions on the blockchain with central bank money.

Key priority 3
Strengthening European and global payments in a dynamic international playing field

The arrival of new players in the payment chain leads to greater competition and innovation, but it also entails risks, including with regard to market power and privacy, and dependence on non-European market players. It places a further strain on the business models of the existing parties in the chain. The Netherlands has an efficient, high-quality payment market, also in comparison with the rest of Europe. This achievement cannot be taken for granted, however. It needs new investment at a time when its income is under pressure from the low interest rate environment and maintenance costs are on the rise. To ensure the smooth operation of the payment system, the Netherlands would benefit from a more European approach. It must be made easy to pay in the same way anywhere in Europe. The European payments system will become stronger if European market players take care of this and we are not dependent on American or Asian players. It will also allow us to better protect the sector from privacy breaches and security issues. That is why we are committed to harmonisation and standardisation, and why we support private initiatives that offer pan-European solutions. We are also actively cooperating in the G20 plan to improve cross-border payments. These payments must become faster, cheaper, more inclusive and more transparent. Stablecoins could also contribute to this, but they also pose many risks. Stablecoins must be regulated appropriately and in line with the risks. Regulating them requires an international approach.

Trends and developments

Banks have traditionally played an important role in the payment infrastructure. The existing players' business models have been under pressure for some time due to the low interest rate environment, the relatively low fees for payment services in the Netherlands and increased competition. The increasing compliance pressure resulting from PSD2 and AML legislation is putting upward pressure on the cost of payments. Margins on traditional banking activities have fallen sharply. Now that market conditions and the ecosystem have changed dramatically, it is even more important to understand where the costs of the payment structure lie and whether this distribution is balanced. We understand and endorse the banks' desire for a new cost-benefit study into the payment system. This study should assess to what extent the sustainability of the Dutch cost model for retail payments is at stake and where the problem areas lie.

New players have entered the payment services market. This promotes competition in the payment market, as well as innovation and the security of payment services. Conventional payment institutions and electronic money institutions have been part of the payment chain for some time. Since PSD2 they have been joined by account information and payment initiation service providers, the latter of which are also payment institutions. Other new entrants are players (such as FinTech companies) operating in niche markets, providers of crypto services and newly formed "challenger banks" or "neobanks", which mostly operate digitally. Some of these new players have become an increasingly important part of the payment chain. Global players (BigTechs) are also becoming more involved in the payment system. Whereas banks have traditionally provided a wide range of services, we are seeing new entrants to the payment market often concentrating on one or just a few services, for example offering competitive foreign exchange rates. The increasing competition is putting further pressure on the already low margins in the payment system.

It is possible that the European Commission's evaluation of PSD2 in 2022 will lead to further standardisation of rules for payment institutions, making the competition among banks even more challenging.

The payment chain is becoming ever more complex and opaque, partly due to increasing fragmentation. Both the retail and wholesale areas are seeing increased fragmentation and outsourcing. The fragmentation is both horizontal and vertical. Growing numbers of players are operating in the same part of the payment system (horizontal fragmentation), while the chain is also growing longer: functions that were previously performed by one party are increasingly carried out by different players (vertical fragmentation). As a result of these trends more players are becoming involved in the provision of payment services. On the one hand this promotes competition and innovation in the payment chain, while on the other hand it leads to reduced transparency, sometimes making it unclear where customers should direct complaints, and increases integrity risks. Fragmentation and outsourcing also impact the robustness of the payment chain (see also key priority 1). Fragmentation also has consequences for the settlement of securities transactions. The fragmentation of central securities depositories (CSDs) means that many intermediaries are required and settlement can be slow.

As well as fragmentation, a simultaneous process of consolidation is under way in the market. A number of mergers and acquisitions have taken place in recent years. Consolidation in the payment chain is aimed at securing a better basis for future growth and strengthening the position in a specific part of the payment system. Further consolidation may benefit cross-border transactions and services: players in domestic markets (such as the Dutch market) are sometimes too small to compete and survive on their own in the European and global financial playing field. Consolidation can contribute to greater efficiency and cost savings. But there are also risks, such as greater dependence on a limited number of players, reduced competition and fewer services geared specifically to local markets. Standard services are becoming the norm.

BigTechs such as Apple and Google have become active in the global payment system in recent years. BigTechs mainly provide payment instruments that allow contactless mobile and online payments by creating a shell around existing payment instruments such as debit or credit cards. They thus function as technical service providers for a licensed operator and enter into partnerships with banks for this purpose. Services such as Apple Pay and Google Pay are also available in the Netherlands and are increasingly used by consumers. BigTechs aim to increase their attractiveness to consumers by making their own ecosystem as attractive as possible in order to retain consumers on their platform. The provision of payment services on e-commerce or social media platforms makes it easy to conduct transactions without leaving the platform, for example. Payment transactions also generate valuable data, which can be used to place more targeted advertisements.[9]

Data are playing an increasingly important role, including in the payment system. New entrants, particularly BigTechs, attach great importance to data collection. Given the growing importance of data use, the value of payment transaction data is also increasing. The downside is that consumers' privacy may be compromised. Questions such as: who has access to my data, is my data secure and will my data only be used for the service for which I have given consent are becoming increasingly important. With payments now being processed by an increasing number of entities it is important to determine which data is required and when, precisely where the data is held and how it is handled.

9 See also DNB (2021) Changing landscape, changing supervision. Developments in the relationship between BigTechs and financial institutions.

Open Finance, which allows regulated exchanges of data between financial and non-financial parties based on customer consent, is expected to lead to greater innovation. The European Commission is due to issue legislative proposals for an Open Finance Framework, resulting from the Digital Finance Strategy and the evaluation of PSD2, in mid-2022. The intention is that this will create an open system in which payment service providers and new entrants can jointly provide new services, sharing data between financial and non-financial players, in accordance with data protection and competition rules. Further standardisation of application programming interfaces (APIs) will also contribute to this. APIs enable systems to communicate and exchange data with each other, so new providers can develop new services using data held by existing parties. If existing parties received remuneration to provide this functionality, they would have a greater incentive to provide smooth access or to continue investing in their API infrastructure. This could help to create a less fragmented API landscape and simplify innovation. The European Commission is also committed to facilitating the interoperability of digital identities (e-ID) to ensure that customers can access financial services quickly and easily and maintain better control of their personal data. If successful, the interoperability of digital identities will further spur innovation and efficiency, including in the payment system.

There is still room for improvement with regard to harmonisation and standardisation in Europe. The creation of the Single Euro Payments Area (SEPA) was an important step in the formation of an integrated European payment market. The aim was to create a single payments area in Europe in which credit transfers would operate everywhere in a similar way, both domestically and across borders. The European payment system remains very fragmented, however, for example in the area of online payments. In the Netherlands, iDEAL is the main method used for online payments, while in Belgium it is Bancontact and in Germany it is Giropay or Sofort, etc. Partly for this reason, various global players, such as American card companies, have been able to secure a major share of the intra-European retail payment market. Further European harmonisation will contribute to the interoperability of payment solutions, so that citizens throughout Europe can pay in the same way, both in stores and online, with the same protection and with a uniform, recognisable payment experience at the lowest possible cost.

A European payment solution will reduce the fragmentation of the European payment system and promote efficiency. A group of European banks has launched the 'European Payment Initiative' (EPI) with the aim of providing a payment solution that can be used throughout the European Union. EPI aims to provide digital payment facilities using instant payments. Since the Netherlands already has a high-quality payment system with low charges, this initiative offers limited added value for the Netherlands in the short term. In the longer term, however, such a European payment solution could compete with the major international card companies and make the European payment market more efficient.

Cross-border payments to and from countries outside the EU and the euro area remain costly, slow, opaque and inefficient. This causes great inconvenience for migrants wishing to send remittances to family members in their country of origin, for example. They pay hefty fees to transfer money and it often takes several days for the money to arrive. Businesses also need faster and cheaper global payments and would benefit particularly from better information (track and trace), standardisation and longer opening hours of payment settlement systems.

The ISO20022 standard, the de facto global financial communications standard, plays a part in simplifying international payments. The ISO20022 standard forms the basis of SEPA and the instant payments system and has been adopted by a number of countries outside Europe. The standard reduces the

risk of errors and enables more information to be included in messages. Banks and businesses have already switched to the ISO standard for their SEPA transfers and direct debits. TARGET2 (for high-value euro payments) and SWIFT (for cross-border payments) will also migrate to this standard in November 2022. It will thus become an important basis for cross-border payments to and from non-EU countries.

The volatility of cryptos makes them unsuitable as a generally accepted means of payment. Cryptos are digital balances or rights that can be transferred and stored electronically using DLT or similar technology. Cryptos enable value to be transferred without the involvement of third parties such as banks or clearing and settlement companies. However, the value of cryptos is by no means guaranteed. Cryptos are therefore used particularly for speculative purposes. In May 2021 the total value of cryptos reached a then record of €2,200 billion. The value subsequently more than halved before surging to a new record high and declining again (see Figure 4). We do not supervise cryptos. Firms providing exchange services between virtual money (crypto) and regular (fiat) money and custodian wallet providers are nevertheless subject to our integrity supervision, as cryptos are vulnerable to financial crime. In addition, some crypto currencies, such as Bitcoin, are based on an energy-intensive algorithm. Our calculations show that the climate impact of Bitcoin in 2020 is estimated at 402 kg of CO_2 per transaction. This is comparable to two-thirds of the monthly emissions of an average Dutch household.[10]

"Cryptos are too volatile to be used as a means of payment"

Stablecoins aim for a stable value, but are not as stable as the name suggests. The issuers of stablecoins endeavour to offer greater price stability by linking them, for example, to a standard currency such as the US dollar, or to gold. This should make stablecoins suitable as a means of payment. A well-known example

Figure 4 Crypto values are very volatile

Total cryptocurrency market cap

Source: Coinmarketcap.com.

10 See DNB Analysis - The carbon footprint of bitcoin (2022)

of a stablecoin is Tether. Stablecoins could contribute to a faster, cheaper and more inclusive global payment system. They also contribute indirectly to innovation in cross-border payments. Traditional players are updating their services and/or reassessing their business model in the light of these developments. Stablecoins also involve risks, however. Although the name suggests otherwise, the value of stablecoins can fluctuate, because the link between stablecoins and fiat currencies is not maintained automatically. Issuers of stablecoins can hold reserves of the currency to which the stablecoin is linked in order to maintain a stable value. In that case, users need to be sure that additional reserves will be held if new stablecoins are issued. As past experience has shown, that promise is not always fulfilled. Users of some stablecoins also have to pay a fee to convert them into euros, for example, or can only convert them in the secondary market, in line with the profit motive of private issuers of stablecoins.

A larger-scale use of new global stablecoins as a means of payment would pose risks to monetary policy, financial stability and competition. At present stablecoins are still used mainly to facilitate trade in volatile cryptos. The extent to which they are currently being used does not yet pose any risks to monetary policy, financial stability and competition. That could soon change, however. The volume in circulation is rising rapidly and interfaces with the mainstream financial system are increasing.[11] Existing parties in the payment system intend to make stablecoins (and other cryptos) accessible to a wider public through their own networks. This could raise interest in stablecoins and their use as a means of payment. Wider acceptance of stablecoins as a direct means of payment could lead to them becoming more integrated in the payment system. There would then be greater financial stability risks and implications for monetary policy. If stablecoins were used for payments on a large scale, any technical outages could make them impossible to convert, for example, leading to economic damage and loss of trust in the payment system. There could also be stablecoin runs (holders of stablecoins seeking *en masse* to redeem them for the collateral) if a stablecoin issuer failed to honour a request to exchange a stablecoin for euros, or if users lost confidence in the issuer's ability to honour such a request. Monetary policy, and the fight against inflation, could also be undermined, because monetary policy is implemented through the banks.

"Stablecoins could contribute to faster, cheaper and more inclusive cross-border payments, but also pose many risks"

Strategy

We support further harmonisation in Europe to promote financial stability, increased efficiency and innovation. The smooth operation of the payment system will benefit from a European approach and European payment solutions that enable users to make payments not only in the Netherlands but also abroad. A private initiative such as EPI could be a useful contribution to this objective. It is in the interest of the Dutch market to support such initiatives so that ultimately it will be possible to compete on a European basis with global players in Asia and the United States, among others, and thus promote an efficient European payment market, even if such initiatives do not immediately improve the efficiency of the Dutch market. We therefore welcome and support initiatives that strengthen the European market.

The Eurosystem itself also has a number of major projects that contribute to the efficiency and integration of the European payment and securities systems. November 2022 is the scheduled go-live date for the consolidation of the TARGET2 high-value payment system and TARGET2-Securities. The new system will then be named T2 and will offer better liquidity management options. A year later, in 2023,

11 See FSB (2022), Assessment of Risks to Financial Stability from Crypto-assets.

this will be followed by ECMS (Eurosystem Collateral Management System), which will largely harmonise the collateral management for national central banks and financial institutions in the context of monetary lending. First, however, the ECB and the national central banks, including DNB, are working hard to enable instant payments through the Eurosystem (TIPS platform) between all banks in the euro area. The first quarter of 2022 marks a major step forward, as all banks must be ready to connect to the platform. Instant payments between euro area countries will then in principle be just as natural as they currently are within the Netherlands. In order to encourage the use of instant payments, the European Commission is expected to propose legislation in 2022 that will require banks that currently offer customers standard European transfers to also offer instant payments. Since instant payments are not yet considered by banks everywhere in Europe to be the "new normal" for credit transfers, many banks offer instant payments as a premium service with fees to match. This is holding back a large-scale introduction of instant payments of the kind seen in the Netherlands. The forthcoming legislative proposal from the European Commission may also address this premium pricing.

We fully support the G20's ambition of making cross-border payments substantially faster, cheaper, more inclusive and more transparent. The world is becoming increasingly international and the payment system must keep up. The G20 declared improved cross-border payments to be a global priority in 2020. This has led to a roadmap with a wide-ranging work programme. We endorse the importance of improving cross-border payments worldwide and are actively participating in various G20 work streams on the implementation of the work programme, which is due to be largely completed by 2027. The processing of cross-border payments should be more comparable to that of domestic payments. That means they should be faster, cheaper, more inclusive and more transparent for individuals and businesses. Meeting these objectives will require extensive cooperation between public and private sectors worldwide.

The regulation of stablecoins should be commensurate with the risks, which depend partly on their adoption as a means of payment.[12] Central banks and supervisory authorities must intervene to mitigate the risks of uncontrolled issuance of stablecoins and safeguard trust in the payment system. Additional safeguards must be put in place, similar to those currently in the mainstream payment system, in case technical faults or cyberattacks make it impossible to exchange stablecoins, for example. The smooth operation of the payment system must never be in question, even in a changing landscape. If the adoption of stablecoins remains limited, a light regulatory regime will suffice, but if adoption increases, stricter regulation is needed. Stablecoins issued by BigTechs could grow rapidly due to the large numbers of consumers that BigTechs are able to reach through their networks.

Stablecoins are borderless, so it is very important that regulation is drawn up on the basis of international coordination. The European Commission is currently working on regulation for cryptocurrencies, including stablecoins. The draft Markets in Crypto Assets Regulation (MiCA) includes rules for crypto issuers and crypto services providers. An important aspect of this draft regulation is supervision of stablecoin reserve management. Components qualifying as payment systems will also be subject to oversight. Crypto payment schemes and crypto wallets will fall within the new PISA[13] framework if they are used for payments on a large scale. Crypto service providers and issuers (including issuers of some stablecoins) will also be covered by the new DORA

12 See Bolt, W., Lubbersen, V. en Wierts, P., Getting the balance right: crypto, stablecoin and CBDC, DNB Working Paper No. 736
13 The new PISA framework was published in November 2021 and sets new requirements for the oversight of electronic payment instruments, schemes and rules. The new framework will replace the existing oversight regulations for payment instruments and comes into force in November 2022.

legislation. Legislation on stablecoins is also being considered in other countries, such as the United States.[14] Regulatory differences should be avoided as far as possible in the interest of global financial stability. Stablecoins could in principle be used worldwide, and a stablecoin user in the United States should have the same rights as in the European Union. International cooperation is therefore essential. The Financial Stability Board (FSB) fulfils an important coordinating role at the international level and sets global standards for the regulation of stablecoins. We participate in the FSB group on Regulatory Issues of Stablecoins (RIS), which was formed to harmonise the international regulation of stablecoins as far as possible. In consultation with other relevant authorities, the FSB will review its previous recommendations on the regulation of stablecoins and consider how to address any remaining gaps. If necessary, the FSB will update its recommendations. It will publish its final report in mid-2023.

We will also issue a publication on new developments relating to stablecoins, cryptos and decentralised finance. We will study the opportunities and risks of new value transfer systems, including cryptos and stablecoins. We will also examine their consequences for the fulfilment of the central bank's remit. The study will focus on factors relevant to value transfers in decentralised networks, networks with intermediaries and hybrids. For example, we will look at transaction validation, privacy and money issuance. The social opportunities and risks will be identified. Finally, policy implications and recommendations will follow, with a focus on risk reduction and the relationship with the digital euro.

14 See for example President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins | U.S. Department of the Treasury.