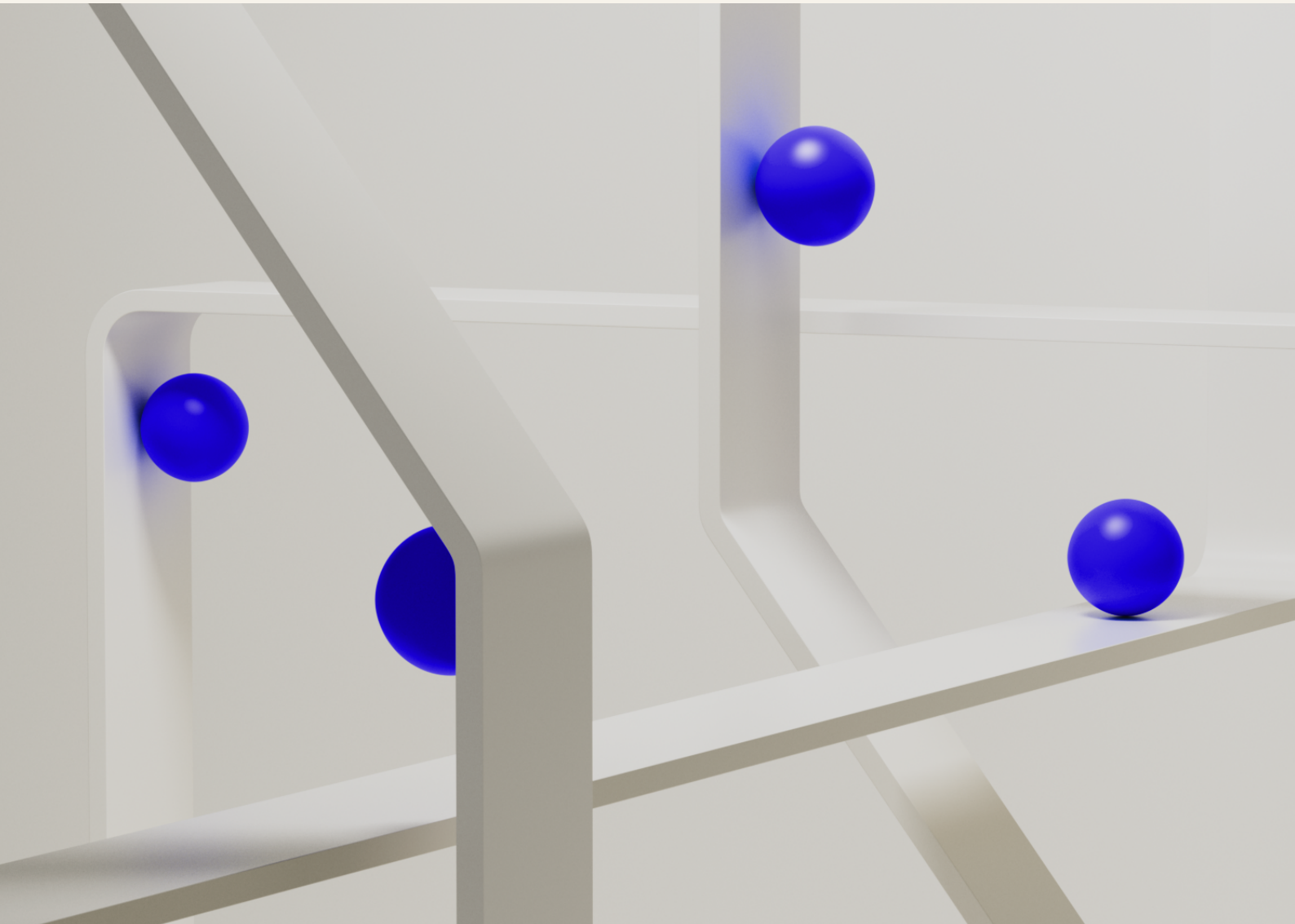
Norges Bank

Financial Infrastructure Report

2026



Selected key figures

NOK 359bn

Daily turnover in Norges Bank's settlement system

95

Number of banks with an account at Norges Bank

NOK 37.7bn

Value of notes and coins in circulation

NOK 9.6m

Daily number of transactions in the Norwegian Interbank Clearing System (NICS)

575 228

Daily number of instant payments

37%

Share of point-of-sale payments made with a mobile phone

Daily turnover in Norges Bank's settlement system: Average for 2025. Source: Norges Bank
Number of banks with an account at Norges Bank: Number of banks with an account at Norges Bank at year-end 2025. Source: Norges Bank
Value of notes and coins in circulation: Value of banknotes in circulation at year-end 2025. Source: Norges Bank
Daily number of transactions in the Norwegian Interbank Clearing System (NICS): Average for 2025. Source: Bits
Daily number of instant payments through NICS Real: Daily average for 2025. Source: Bits
Share of point-of-sale payments made with a mobile phone : Survey conducted in spring 2026. Source: Norges Bank

Norges Bank's Financial Infrastructure Report

In its annual Financial Infrastructure Report, Norges Bank discusses developments, vulnerabilities and risks in the financial infrastructure. The *Report* is a part of Norges Bank's work to promote financial stability and contribute to an efficient and secure financial infrastructure.

Norges Bank's other reports on financial stability

In its bi-annual Financial Stability Report, Norges Bank assesses the prospects for financial stability. The *Report* discusses cyclical and structural trends in banks, other financial institutions, the financial markets and the Norwegian economy that are of importance for vulnerabilities and risks in the financial sector.

Norway's financial system is published annually and provides a comprehensive overview of Norway's financial system, its tasks and the performance of these tasks.

Contents

Editor: Ida Wolden Bache

The report was published on 10 June 2026 and is available at www.norges-bank.no

Executive Board's assessment

Norway has an efficient and secure payment system. Operations are stable and payments can be made swiftly at low economic cost and in ways that are adapted to users' needs.

At the same time, according to threat assessments, Norway is facing the gravest security policy situation since the Second World War. Geopolitical tension increases the risk of hostile actors attempting to exploit vulnerabilities. Technological advances, in particular within the fields of artificial intelligence and quantum technology, also contribute to a more demanding threat landscape. Mitigating vulnerabilities and ensuring sufficient resilience going forward will require systematic work and a long-term perspective.

Resilience must be strengthened
Financial sector entities are making a considerable effort to increase the resilience of their own systems, and continuing this work is important.

Threat-led penetration testing helps identify and patch vulnerabilities before attackers can exploit them. With the coming into force of the Digital Operational Resilience Act (DORA), systemically important financial entities are required to conduct such tests of their systems and processes. Sharing lessons learned in the tests across the financial sector helps increase the resilience of the financial infrastructure overall.

The emergence of increasingly powerful artificial intelligence (AI) models is altering the cybersecurity risk landscape, particularly by increasing the speed and scale at which software vulnerabilities can be identified. AI tools give attackers greater opportunities for exploiting security vulnerabilities before they are patched, but, in time, they may strengthen defences by contributing to more efficient patching. This development forces system owners to update their systems more frequently and rapidly. This also creates a greater need to maintain a sound overview of IT systems. Well-established measures such as system monitoring and more frequent security testing mitigate risk.

Over time, the emergence of quantum computing may pose a threat to financial infrastructure security mechanisms. Post-quantum cryptography will therefore have to be implemented, and this work will be

extensive. Individual entities are responsible for securing their own systems, but coordination is important to ensure that the financial infrastructure overall is sufficiently secure. Industry federation Finance Norway's advice to the financial sector on how to manage AI and quantum technology developments helps ensure a coordinated sector response.

Cooperation must be strengthened

The financial infrastructure is made up of many participants and systems that need to operate together in order to function. Harmonisation of systems, operational frameworks and procedures across borders can provide substantial efficiency gains but requires close coordination and a joint effort. The work to introduce a shorter securities settlement cycle (T+1) across Europe by 11 October 2027 highlights this need.

Norges Bank is of the opinion that collaboration with Nordic and other European central banks is the best choice for secure and stable operation of the settlement system in the long term. Integration of NOK into the European TARGET Instant Payment Settlement (TIPS) system is ongoing. In parallel, work on the necessary clarifications for Norwegian participation in T2 is ongoing.

It is important to maintain critical financial infrastructure functions, also in times of crisis, war or conflict. Identifying fundamental national functions pursuant to the Security Act provides important insights into critical functions and the entities that support them. Nevertheless, Norges Bank considers that a broader review is needed to evaluate whether there is sufficient governance capacity and operational autonomy for critical functions in the financial sector in times of peace, crisis and war. Such a review should also include dependencies and concentration risk. It could also provide a better basis for assessing the need for measures, such as independent contingency solutions. Such a review could also provide the authorities with a better basis for assessing the consequences of potential changes, such as mergers and acquisitions.

The financial infrastructure will be more secure with more payment channels.

In Norway, the authorities and the financial industry collaborate on how payment system contingency arrangements should be strengthened to withstand more serious incidents. This collaboration has resulted in a number of recommended measures covering the entire payment chain, including banks, clearing and settlement systems, points of sale and households. Work is currently under way to implement these measures, and it is important that this work continues to be prioritised.

The financial infrastructure becomes more secure and efficient when multiple payment channels are available and sound contingency arrangements are in place in the event of disruptions in one or more links in the chain. Authorities, the financial industry and users all contribute to stronger contingency measures and lower risk by making alternative

payment channels available, establishing independent contingency arrangements and maintaining sound individual preparedness.

One of the measures completed in spring 2026 was an update of the recommendations on individual payment preparedness, which now also includes recommendations for individual preparedness for points of sale. A key recommendation is that both payers and payees should be able to use several different forms of payment. The increasing importance of mobile payments suggests that mobile-based payment solutions should also support multiple underlying payment channels.

Cash is still needed

Cash still plays an important role in the payment system, particularly for contingency preparedness and financial inclusion, although the system is primarily secured through effective and secure digital solutions. Cash is used for a small share of the total number of payments. At the same time, a survey conducted for Norges Bank shows that a quarter of the population uses cash at least every month. The same survey shows that a clear majority considers that the opportunity to withdraw and deposit cash is important.

Norges Bank has undertaken a new assessment of the denomination structure and has decided to retain the current structure but to stop supplying new 1000-krone banknotes. The 1000-krone note currently accounts for a limited share of the number of banknotes in circulation and, in a normal situation, is not materially significant for cash payment efficiency. However, in a serious contingency situation, the note could play an important role. Norges Bank can put more of the note into circulation if necessary.

For cash to fulfil its functions, the public must be sufficiently able to access and use cash, and businesses must be able to access change and to deposit cash revenue. Banks are statutorily obligated to provide customers with sufficient cash services. Most cash handling services are carried out by non-banks. Norges Bank emphasises that banks' responsibility applies regardless of a well-functioning service provider market.

Current provision of cash services is vulnerable and has certain weaknesses. If banks do not ensure satisfactory solutions themselves, Norges Bank is of the opinion that more detailed regulation should be drawn up.

Research into tokenisation and central bank digital currency is continuing

Norges Bank has assessed whether introducing a central bank digital currency (CBDC) is appropriate to ensure that paying with the Norwegian krone will remain secure, efficient and attractive. The Bank has concluded that introducing such a currency is currently not warranted. The introduction of a CBDC is not currently the measure most conducive

to promoting payment system innovation, strengthening contingency preparedness or otherwise contributing to a more efficient and secure payment system. At the same time, financial system technology is advancing rapidly, and new services and participants are emerging. Tokenisation enables innovation and efficiency gains and allows for lower settlement risk. Should tokenised transactions become more common, a need to introduce solutions for central bank money settlement of such transactions may arise. However, there are several aspects of tokenisation that must be clarified. Norges Bank will continue to research tokenisation and CBDC in order to be able to introduce a CBDC should it become necessary. Norges Bank will expand its collaboration with financial market participants on technical testing.

The ECB's work to develop a retail CBDC – a digital euro – is at an advanced stage. The ECB states that if necessary regulation is adopted in the EU in 2026, a digital euro can be introduced in 2029. The ECB and the Eurosystem are also exploring and testing central bank money settlement solutions for transactions and trades in tokenised assets. These solutions may be relevant as infrastructure for new forms of payment and settlement in NOK should the need arise and Norges Bank enter into an agreement to use the European settlement system T2.

Stablecoins fall short as a means of payment alternative

Stablecoins are a tokenised means of payment alternative that use open blockchains as their transaction infrastructure. Currently, the use of stablecoins is predominantly linked to cryptoasset investment, but various niche applications are growing, including international payments and payments requiring programmability. Stablecoins may provide benefits for such niche applications, but at the same time lack some of the characteristics of general-purpose means of payment. For example, stablecoins have been subject to fluctuations in value. New regulation makes stablecoins more resilient to falls in value as a result of loss of confidence, but market frictions could still lead to fluctuations in value that are unacceptable for general-purpose means of payment and systemically important settlement. In addition, use of open blockchains currently does not provide users with the security provided by existing frameworks for traditional payments.

The Executive Board

19 May 2026

An efficient payment system

The Norwegian financial infrastructure is efficient, with stable operations and few disruptions. Payments can be made swiftly at low economic cost and in ways that are adapted to users' needs.

International harmonisation, adaptation to amended standards and technological developments are important drivers of further development. This section discusses some of the main aspects of payment operations and the recent development of key components in the financial infrastructure.

Norges Bank's settlement system

Norges Bank's settlement system (NBO) is the core of the Norwegian payment system, and most electronic payments made in NOK are ultimately settled between banks in this system. Norges Bank is the operator of NBO.

The current settlement system is efficient, and operations in 2025 were stable without material disruptions. At the end of 2025, a total of 103 banks and other financial institutions held an account in NBO, down from 112 in 2024. In 2025, average daily turnover in NBO increased by NOK 9bn to NOK 359bn. At year-end 2025, banks' sight deposits and reserve deposits totalled NOK 37bn.

The work to modernise NBO continued in 2025. A key milestone was the transition to the ISO 20022 standard for payment messages, which facilitates more efficient collaboration and development of settlement systems in line with international requirements. The new format was first used for gross payments in March, then in securities settlement and, in November, for net payments. The migration was performed in collaboration with NBO participants and also included adaptations in participants' own systems and processes to satisfy the requirements of the new standard. Settlement system operation using the new message format has been stable after production rollout. The transition to ISO 20022 involves regular upgrades of the settlement system ahead in line with new versions of the message standard. Bits AS has decided that the Norwegian Interbank Clearing System (see also mention below) will not be developed to receive and process ISO 20022 based transactions. This

has resulted in an increase in the number of transactions sent to NBO from a daily average of 4 595 in 2024 to 13 577 in 2025. For more details on NBO, see the Norges Bank's Settlement System Annual Report.

Norges Bank has continued to work on the next generation settlement system. Work on necessary clarifications for participation in the Eurosystem's settlement service, T2, as a platform for NBO RTGS is ongoing. The work includes assessments of security, national control and contingency solution requirements. A final decision will be made once necessary clarifications have been addressed.

Norges Bank has also continued work to establish a new service for instant payments in NOK (NBO INST) using the Eurosystem's TIPS solution as a platform. Using TIPS will require more comprehensive adaptations than previously assumed, and the progress plan is currently being revised in close collaboration with the ECB and the banking sector in Norway.

Norwegian interbank clearing system

The Norwegian interbank clearing system (NICS) is banks' joint system for receiving and clearing interbank payment transactions before they are settled with finality in NBO. Norges Bank has awarded the licence to operate NICS to the financial industry's infrastructure company Bits, and Norges Bank supervises NICS. Bits has entered into an agreement with Mastercard Payment Services Infrastructure (MPSI) for the technical operation and management of NICS. Bits is the system owner and responsible for the system, including the parts outsourced to MPSI.

NICS operations were stable in 2025. There were some operational disruptions that resulted in clearing delays, but the incidents were resolved and settlement completed the same day.

A total of 95 banks participate in NICS. The total amount cleared in NICS fell by 35.7% in 2025, to a daily average of NOK 261bn, reflecting the discontinuation of SWIFT-format transaction processing in September 2025. Such transactions are now sent directly from banks to NBO. In August 2025, all the banks had redirected their transactions.

Securities settlement and central counterparties

Securities settlement in NOK involves the delivery of securities in accounts at the central securities depository (CSD) and payments made via designated accounts in NBO. To eliminate settlement risk, the seller's transfer of securities is coordinated with the buyer's payment through the systems of Norges Bank and the CSD. The Norwegian CSD is operated by Euronext Securities Oslo.

Swifter securities settlement in Europe

Currently, securities transactions must be settled within two days (T+2). The forthcoming requirement of settlement within one business day of the trade (T+1) entails extensive change in the securities market.

The European Commission and the European Securities and Markets Authority (ESMA) have planned that the whole of the EU will transition to T+1 by 11 October 2027. Finanstilsynet (Financial Supervisory Authority of Norway) is following up on this as an EEA-relevant regulatory framework, and a legislative amendment was circulated for consultation in spring 2026. Switzerland and the UK will also implement T+1 at the same time as the EU. The introduction of the T+1 requirement in Europe follows the introduction of similar requirements in the US and Canada in 2024.

The purpose of the shorter settlement cycle includes reducing counterparty risk and margin requirements. The transition will make securities settlement more efficient but will also require resource-intensive changes in operating schedules, procedures and technical infrastructure throughout the securities market. The transition will also have implications for clearing in NICS and securities settlement in NBO and Euronext Securities Oslo, with extended opening hours and more clearings and securities settlements over the course of the day.

At the end of 2025, the total value of securities registered in the CSD amounted to NOK 7 698bn. System availability was high in 2025. Two incidents caused disruptions to securities settlement but had only limited consequences. Measures have been implemented to reduce the risk of similar incidents.

Euronext Securities Oslo is part of a corporate group that includes several other CSDs in Europe. Euronext is undertaking a modernisation project aimed at increasing harmonisation across different CSDs and jurisdictions. The solution under development is designed to align with the ECB's securities settlement platform, T2S. Should Norges Bank decide to join T2, the question of whether to join T2S will also become relevant.

To protect against potential counterparty issues during the period from which a trade is agreed upon and until settlement is made, many trades are settled through a central counterparty (CCP). The use of CCPs results in positions that must be settled in the Norwegian securities settlement system. The CCPs most commonly used by Norwegian participants at present are Cboe Clear Europe (CCE), SIX x-clear, Euronext CCP and LCH Ltd. The latter, based in the UK, is particularly widely used.

Foreign exchange settlement

In a foreign exchange (FX) transaction, parties exchange two currencies. This market is dominated by the largest international banks. In traditional FX settlement, there is a risk that the counterparty will fail to fulfil its part of the agreement. The US Continuous Linked Settlement (CLS) system was set up in 2002 to reduce FX settlement risk.

Globally, CLS manages FX transaction settlement in 18 currencies. 75 of the world's largest banks settle their own transactions as well as transactions for 38 000 indirect participants. An average of USD 8 000bn in transactions are settled daily. CLS has persistently delivered very stable services, and 2025 was no exception.

Prior to settlement, all participants' liquidity needs in the form of net positions for each currency are calculated on the basis of submitted transactions. This reduces the liquidity needs of participating banks by more than 95%. In 2025, banks settled FX trades, including NOK trades, through CLS, amounting to a daily average of NOK 819bn. Payment obligations to CLS were reduced to a daily average of NOK 28bn through netting.

Settlement of FX transactions involving NOK takes place via CLS' account at Norges Bank. CLS participant banks transfer their payment obligations and receive their claims in NOK via this account. To ease banks' access to liquidity, Sveriges Riksbank, Danmarks Nationalbank and Norges Bank have established the Scandinavian Cash Pool, providing CLS participant banks with the opportunity to borrow in SEK, DKK and NOK against deposits held in any of the three central banks.

Electronic retail payment services

Electronic retail payment services include payments using bank deposits via payment instruments such as payment cards and account-to-account (A2A) transfers. The Financial Supervisory Authority of Norway is responsible for supervising and overseeing retail payment services systems and regularly publishes reports on their condition. Norges Bank monitors developments in the use of different means of payment and payment instruments in retail payment services.

Payment methods have changed considerably in recent years. Most payments still take place at physical points of sale, but online shopping accounts for an increasing share of the total. From 2024 to 2025, the use of mobile payments increased substantially, both at physical points of sale and for online purchases. The annual report Retail Payment Services provides details on developments.

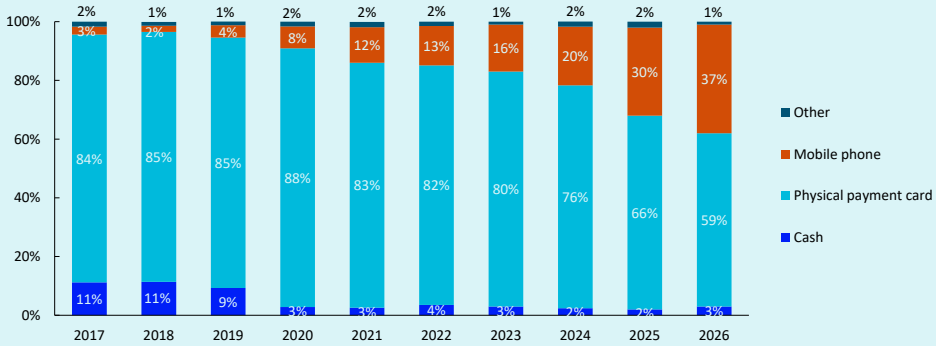
Mobile payments in shops continue to rise

More new solutions for mobile payment in shops have become available in recent years. In August 2024, a new solution for payment in NorgesGruppen's chains of stores, Trumf Pay, was launched. In December 2024, payment and ID solutions company Vipps launched its new solution for NFC payments at physical payment terminals, Vipps NFC. In December 2024, banking groups DNB and Eika-Gruppen enabled Apple Pay for their customers. In summer 2025, Apple Pay was made available for banking group Sparebank 1's customers. Developments have previously been described in more detail in Norges Bank (2025a).

Norges Bank (2025a) anticipated that the launch of these solutions would boost mobile payments at points of sale further. Data showing recent developments are now available. Chart A.1 shows responses from Norges Bank's surveys. The share of mobile payments at points of sale increased from 30% in March 2025 to 37% in March 2026. These figures include both terminal-based and online mobile payments. Terminal-based mobile payments alone increased from 12% in 2024 to 27% in 2025.

In 2024, national payment system BankAxept's share of Norwegian card payments fell below 50% for the first time since the system was established in the early 1990s. Much of the decline can be attributed to strong growth in online shopping and card use abroad, areas where BankAxept is not available. However, relative use in BankAxept's core area, card payments at physical points of sale, has also declined, largely due to the rapid rise in mobile payments. Until 2024, only cards from international card networks, such as Visa and Mastercard, were the underlying payment instruments for such payments.

Chart A.1 Payment methods at points of sale
In percent of the total number of payments



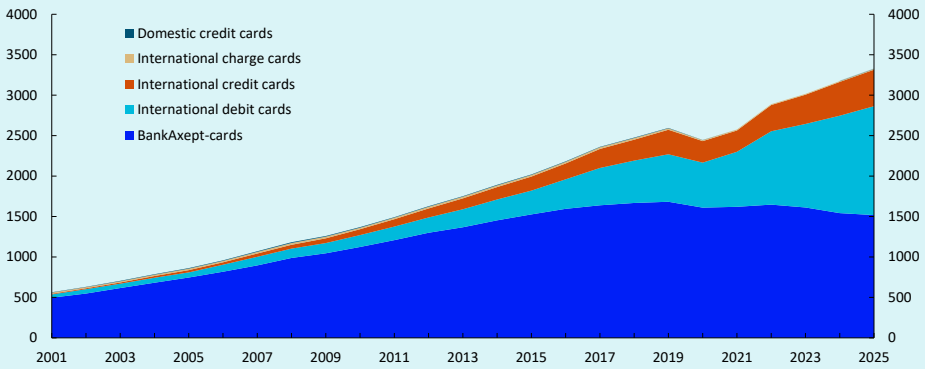
Source: Norges Bank

From spring 2024, BankAxept was gradually made available in Apple Pay, which became available to customers of DNB and Eika-Gruppen in December 2024 and to Sparebank 1 customers in June 2025. From December 2024, BankAxept was available in Vipps NFC.

Usage of the different card networks not only depends on availability, but also on the choices made by payers and payees. BankAxept is mainly available only via co-badged cards, usually Visa debit cards. When co-badged cards, either digital on a mobile phone or physical, are used at terminals, the point of sale selects the card payment network, but the payer can override the selection. Most of these payments are likely made through the BankAxept network as this is the least expensive option for the point of sale in many cases. The international card networks also provide credit cards, which are non-co-badged cards.

BankAxept usage continued to fall in 2025 (Chart A.2). BankAxept's share of total card payments also declined, from 49% in 2024 to 46% in 2025. BankAxept's share of card payments is higher if only payments at physical payment terminals in Norway are included, but this share is also declining. The market share for this segment fell from 74% in 2024 to 70% in 2025. The decline may be due to a number of circumstances. For example, not all banks have facilitated mobile payments with BankAxept, nor is BankAxept available for NFC-based mobile payment solutions other than Apple Pay and Vipps NFC, such as Google Pay and Samsung Pay.

Chart A.2 Use of Norwegian payment cards.
By issuer and function. In millions of transactions



Source: Norges Bank

Cash

Norges Bank is responsible for meeting public demand for cash by supplying banks with cash, both in normal times and times of crisis.

The amount of cash in circulation depends on its use as a means of payment and a store of value but also on cash infrastructure and circulation patterns. The nominal value of cash in circulation was stable from 2006 to 2015 but declined by one fourth from 2016 and 2025. The average value of banknotes in circulation in 2025 was NOK 33.6bn, a decline of NOK 0.8bn (2.2%) from 2024. The average nominal value of coins in circulation declined from NOK 4.19bn in 2024 to NOK 4.14bn in 2025 (1.3%).

The real value of cash in circulation has also declined considerably over the same period. In 2025, cash in circulation relative to mainland GDP and private consumption was 0.9% and 1.7%, respectively. This is somewhat lower than in 2024, and halved since 2016. The cash share of the general public's means of payment holdings (M1) has also fallen steadily over time and was 1.3% in 2025, and 2,7% in 2016. This is very low compared with most other countries with available statistics. Developments in and composition of banknotes and coins in circulation is discussed in greater depth in the annual report Årsrapport sedler og mynter 2025 (in Norwegian only). You can also see Notes and coins – statistics.

The amount of cash in circulation does not indicate how often it is used for payments or by whom. Norges Bank conducts an annual payment survey, where respondents are asked how they paid when last making a purchase at a physical point of sale or making a payment to a private individual. This survey has shown a decline over time in the cash share of payments, and the share has been at around 3% since 2020. In December 2025, Norges Bank conducted a somewhat more extensive survey about cash among consumers. The results showed that 25% of the respondents used cash at least every month. The role of cash in the payment system is discussed in more detail in the article "Cash is still needed", and the use of cash services in the Retail Payment Services annual report.

A secure payment system

Norway has a secure payment system, but an escalating threat landscape increases the risk of serious incidents. Strengthening security and contingency arrangements in the payment system must therefore be a priority.

The security and contingency arrangements of individual entities are the first line of defence in the payment system and the financial infrastructure as a whole. Both the authorities and private sector participants are acutely aware of risk, vulnerabilities and the need for systematic security and contingency planning. There are stringent requirements for safeguards and testing and for continuity and backup solutions. Exercises are conducted regularly, and effective coordination across the sector contributes to sound incident management. All of these elements have strengthened financial infrastructure resilience. Adverse incidents and attacks have rarely resulted in severe consequences. However, for this to remain the case in the future, security and contingency arrangements must be strengthened further.

A demanding threat landscape requires measures across several fronts

Open threat assessments from Nordic Financial CERT, the Norwegian Intelligence Service, the Norwegian Police Security Service and the Norwegian National Security Authority (NSM) show that Norway in 2026 faces the gravest security policy situation since the Second World War. According to the threat assessments, hybrid threats – combined digital and physical attacks – are in particular becoming increasingly relevant. Hostile states and organised criminals are expanding their intelligence activities and have growing capability and willingness to carry out sabotage and influence operations, including against Norwegian interests. Given their role in managing substantial assets and operating critical societal functions, banks and other key financial infrastructure entities are attractive targets.

Geopolitical tensions are now also affecting areas previously regarded as stable. When major powers challenge international rules and agreements, this can disrupt trade, financial markets and the financial

infrastructure. While decades of globalisation and integration have generated benefits, they have also created cross-border dependencies that can be exploited for political leverage.

Financial infrastructure vulnerabilities (see box) build up over time, but risks may materialise abruptly. Recent developments have brought

Vulnerabilities in the financial infrastructure

Many dependencies
The financial infrastructure comprises many components that are dependent on each other and on underlying infrastructure such as electricity supply and electronic communication. Digitalisation and system integration have provided efficient payment services that make it possible to make payments quickly, at low cost and adapted to users' needs and preferences.

At the same time, this implies that the failure of critical components can rapidly have major consequences. In severe crisis scenarios involving sabotage, natural disasters or war, even well-protected systems may become unavailable. Owing to the complexity arising from a large number of systems and interdependencies in payment chains, together with the associated complex supply chains, the number of potential attack surfaces also increases. Geopolitical tension increases the risk that cross-border dependencies may be exploited for political leverage.

Extensive outsourcing
The financial sector outsources many services and tasks, often with the aim of more cost-efficient and robust solutions. Economies of scale in system operations and external expertise naturally lead to consolidation and concentration in the market for these services.

At the same time, a higher degree of outsourcing and concentration constitutes a system-level vulnerability when many entities use the same software, hardware and system platforms. Several critical functions in the financial infrastructure depend on a small number of providers of cloud services, system software and core systems.

In pace with stronger market concentration in the provider market, providers' corporate structures have become more complex and often consist of a number of subsidiaries that may be subject to regulation in different jurisdictions. This makes it difficult for authorities and system operators to maintain an overview of providers' risk exposure as regards technological security, personnel security and regulatory changes in providers' home countries.

Attractive targets
As custodians and transfer agentsof substantial assets, banks, key market participants and financial market infrastructures (FMIs) in the Norwegian financial system are attractive targets for a wide range of threat actors.

Digital profit-motivated crime is on the rise, and organised crime constitutes a significant threat to financial institutions and their customers. Criminals steal card information, identities, access and other sensitive and valuable data. A more tense geopolitical environment also means that complex threats, with collaboration between state and criminal actors, occur more frequently. While technological advances such as artificial intelligence are providing attackers with new tools, they may also provide new defensive capabilities.

particular attention to risks associated with dependencies on global technology providers. As one of the world's most digitalised societies, many critical functions in Norway depend on global providers and system platforms. Norwegian financial entities have limited ability to influence how these global entities operate. The ability to replace them within a reasonable timeframe is also limited if they discontinue or restrict their services in Norway.

Reducing risks associated with vulnerabilities requires systematic and long-term efforts across several fronts:

- **Increased resilience:** Continually strengthening existing systems remains important, including through advanced threat-based testing.
- **Cooperation:** To address both threats and opportunities in an integrated international financial infrastructure, cooperation at the national level and with close allies in the Nordic region and Europe must be strengthened.
- **Diversification:** Authorities, the financial industry and users all play important roles in reducing risk by making alternative payment channels available, establishing independent contingency arrangements and maintaining sound self-preparedness.

Increased resilience

The work to strengthen the resilience of existing systems must be continued. Financial sector entities are making a considerable effort to increase the resilience of their own systems. Threat-led Penetration testing (TLPT) are demanding tests during which critical functions, together with associated systems and processes within each entity, are exposed to realistic attacks carried out by advanced attackers. The realistic nature of these tests provides valuable lessons and system-specific insights that can be quickly applied to address vulnerabilities and strengthen security and contingency arrangements.

With the introduction of the Digital Operational Resilience Act (DORA), TLPT was made mandatory for designated entities, including requirements regarding testing frequency and reporting.

Under DORA, entities are designated by Finanstilsynet on the basis of quantitative or qualitative criteria, with input from Norges Bank. In spring 2026, Finanstilsynet designated the organisations initially subject to the requirement, and Norges Bank is in the process of planning testing in cooperation with the designated entities. The entities prioritised are the 15–20 largest in the financial sector with responsibility for critical infrastructure.

The European TIBER framework provides guidelines and guidance for the implementation of TLPT tests. Finanstilsynet and Norges Bank have cooperated on the implementation of this framework in Norway,

TIBER-NO. In addition to those entities that were already invited to voluntary testing in TIBER-NO, the introduction of DORA also requires TLPT testing of the largest insurance companies.

Norges Bank assists organisations with planning, coordinating involved entities, conducting risk assessments and executing and evaluating TIBER tests. An important part of the work is to facilitate the sharing of experience between entities that have conducted such tests. Through the TIBER Forum, participants can exchange information and experience related to TIBER testing in a confidential environment for discussing relevant and sensitive issues.

By sharing these insights, others can benefit and address potential vulnerabilities within their own operations before they can be exploited by threat actors. This strengthens overall financial infrastructure resilience. Some of the general lessons learned so far include:

- The security level is persistently high, especially in systems exposed to the internet. However, the level is not always as high behind defensive perimeters. In such cases, entities may be vulnerable to attackers escalating their own access or moving laterally within IT systems.
- In the tests, social engineering is used via email, SMS or phone calls to assess how attackers can exploit human vulnerabilities. Such attacks can be very difficult to detect. Social media such as LinkedIn may make it easier to identify key individuals with access to the most sensitive systems and to target them.
- Entities invest heavily in security technology, but this technology is not always sufficiently adapted to their specific IT environment. Insufficient adaptation of configurations weakens the ability to detect warning signals of cyberattacks and may create a false sense of security.
- The tests have revealed concentration risk related to the widespread use of the same security service providers and security software across entities. When many actors rely on similar solutions, vulnerabilities may have broader consequences than for the individual entity. This may create significant challenges if multiple customers of a provider are affected by an attack at the same time, for example if incident management, support and recovery become bottlenecks.
- Firms with fragmented IT environments often have weaker overall security. A large and complex system portfolio increases the attack surface, while also making security work more demanding to scale and prioritise. Firms with more centralised and harmonised solutions are therefore often better equipped.

The emergence of increasingly powerful AI models is altering the cybersecurity risk landscape, particularly by increasing the speed and scale at which software vulnerabilities can be identified and exploited. This is a development that has been observed over time, but which has

been brought into sharper focus with the introduction of new, advanced AI models such as Claude Mythos.

Such advanced models have until recently primarily been available to a limited number of entities, particularly large international technology companies. This may strengthen the security of their systems but at the same time reinforce dependencies and concentration risk associated with a small number of global technology companies.

The new models have proven their ability to quickly analyse large data volumes and have been able to identify so-called zero-day vulnerabilities, ie vulnerabilities unknown to the providers of the software. Wider availability of such tools increases the risk that vulnerabilities may be exploited before they are patched. At the same time, the technology provides new opportunities to strengthen cybersecurity, including through improved monitoring, automated testing and faster remediation. This may strengthen system resilience over time.

In the near term, developments may lead to increased frequency, pace and scale of cyberattacks. In many cases, system owners will have less time to identify and address vulnerabilities. This increases the need for a comprehensive overview of own systems and supply chains, rapid response to incidents and robust continuity and recovery solutions.

This development is global and affects all sectors. Efforts are under way at both national and international levels to establish shared situational awareness and strengthen response coordination. Recommendations from Finance Norway support a coordinated approach to managing AI-related cyber risk in the financial sector. For Norges Bank, this means that efforts to strengthen payment and settlement system resilience are highly prioritised. Emphasis is placed on early identification of vulnerabilities, clear requirements for service providers and follow-up through monitoring and supervision.

Cryptography is another issue affecting the resilience of existing systems. Fundamental security protocols in the financial infrastructure are largely based on cryptographic algorithms that have been considered secure for decades. However, over time, the emergence of cryptographically relevant quantum computing may pose a threat to these security protocols. The transition to post-quantum cryptography (PQC) in financial infrastructure is an extensive undertaking, but, unlike many earlier cryptographic challenges that often had to be addressed at short notice, this transition is planned and gradual. Important progress has already been made, but the work is far from done. See “Quantum computing threats and financial system measures” for more details.

Strengthened national and international collaboration

The financial infrastructure is about national and international interaction, which is critical for both efficiency and security. Collaboration between entities strengthens defences, and the development of alternative payment channels and contingency arrangements takes place through interaction between the industry and the authorities. Effective incident management also requires close collaboration and coordination, as integration of different systems and entities means that incidents can quickly have major consequences across organisations and borders.

In Norway, the authorities and the financial industry have long cooperated on contingency arrangements and incident management. The Financial Infrastructure Crisis Preparedness Committee (BFI) was established in 2000 to bring together relevant actors in Norway in the event of a major incident, as well as to exchange information and coordinate responses. Through the BFI, the authorities and the industry also meet regularly for joint exercises. In 2025, the BFI participated in the cross-sector exercise Digital 2025, which included the simulation of a large-scale cyberattack on the financial sector and served as preparation for the national exercise programme "Totalforsvarsåret 2026" [Total Defence Year 2026]. This programme aims to strengthen Norway's ability to prevent and manage the effects of security policy crises and war through a range of activities. The financial sector, both the authorities and the industry, participates in this effort.

In its white paper on total preparedness, the Norwegian government announced that a new council structure would be established for the ministries' work related to preparedness planning and status assessments in civilian sectors. Financial services is one of the sectors for which such a council will be established. The Ministry of Finance is currently assessing, in consultation with Finanstilsynet and Norges Bank, how the purpose of preparedness councils can best be achieved in the financial sector, including the extent to which existing council structures, such as the Preparedness Committee for Financial Infrastructure, can be further developed.

The Nordic Financial CERT (NFCERT) supports Nordic financial institutions in the analysis and management of digital attacks. A substantial share of institutions in the Norwegian financial sector are members of NFCERT, including Norges Bank. Broad and active participation in NFCERT strengthens the financial sector and the financial infrastructure. Together with Finanstilsynet, NFCERT serves as the sectoral response function for IT security incidents and, like Norges Bank, is a partner in the Norwegian National Cyber Security Centre.

To enhance assessments of systemic IT risks that may threaten financial stability, Finanstilsynet and Norges Bank have established a joint analysis

group that also includes other key financial system participants. The group has developed a method for such assessments, based on a model developed by the European Systemic Cyber Group (ESCG). In 2025, a pilot was conducted to test the method. Finanstilsynet and Norges Bank decided in 2026 to continue their collaboration in the analysis group.

Collaboration and dialogue are not limited to contingency arrangements. The Payment Forum brings together a broad set of stakeholders in the payment system: authorities, the financial industry and representatives of consumers and non-financial firms. The purpose of the forum is to exchange information on current issues and to discuss proposals for payment system improvements.

International collaboration has also been strengthened. Several fora have now been established to exchange information and coordinate cross-border response between authorities. The EU Systemic Cyber Incident Coordination Framework (EU-SCICF) was established in November 2024 through Article 49 of the EU's DORA Regulation and was implemented in Norway on 1 July 2025. The Working Group on Operational Resilience (WGOR) was established in 2025 as a new collaboration forum under the Nordic Baltic Stability Group (NBSG) and provides Nordic-Baltic authorities with a platform to coordinate their activities within the EU-SCICF and conduct joint exercises. Through NFCERT, the Nordic financial industry has established a well-functioning collaboration on threat intelligence, information management and incident management.

Cross-border harmonisation of systems, operational frameworks and procedures can provide substantial efficiency gains. External expertise and robust systems located abroad can make valuable contributions to strengthening operations, development and security in the Norwegian financial infrastructure. Norges Bank's is of the opinion that collaboration between Nordic and other European central banks is the best long-term option for the secure and stable operation of the settlement system. Integration of NOK into the European TARGET Instant Payment Settlement (TIPS) system is ongoing but requires more extensive adaptation than originally assumed. As a result, the timeline has been revised. In parallel, work on the necessary clarifications for possible Norwegian participation in T2 is ongoing.

While collaboration with external partners is a strength, maintaining the capacity to operate independently is essential. If local expertise becomes insufficient and distance to the operation and development of critical systems becomes too great, local ability to govern and control deliveries may be weakened. With heightened geopolitical tension, reliance on foreign resources may become a severe vulnerability. Foreign ownership, offshored services and dependence on key foreign resources may weaken the governance capacity and operational autonomy of Norwegian entities, particularly in times of crisis, war or conflict.

It is important to maintain critical financial infrastructure functions, also in times of crisis, war or conflict. Identifying fundamental national functions pursuant to the Security Act provides important insights into critical functions and the entities that support them. Nevertheless, Norges Bank considers that a broader review is needed to evaluate whether there is sufficient governance capacity and operational autonomy for critical functions in the financial sector in times of peace, crisis and war. Such a review should also include dependencies and concentration risk. It could also provide a better basis for assessing the need for measures, such as independent contingency solutions. Such a review could also provide the authorities with a better basis for assessing the consequences of potential changes, such as mergers and acquisitions.

The data basis for such mapping will improve over time. Entities subject to DORA are now required to maintain a register of ICT service contracts (RoI) and the register must be reported to Finanstilsynet. The register must include all IT service contracts and specify, among other things, critical or important contracts. The deadline for reporting contracts to the register was 13 March 2026. In line with DORA, a register will also be established at a European level.

Security and efficiency through diversification

The financial infrastructure becomes more secure and efficient when multiple payment channels are available and sound contingency arrangements are in place in the event of disruptions in one or more links in the chain.

In Norway, the authorities and the financial industry collaborate on how payment system contingency arrangements should be strengthened to withstand more serious incidents. This collaboration has resulted in a number of recommended measures covering the entire payment chain, including banks, clearing and settlement systems, points of sale and households. Many of these measures involve strengthening existing backup solutions or establishing new ones. Through 2025 and 2026, the Ministry of Finance has held several meetings and received reports from the financial industry, Norges Bank and Finanstilsynet on the implementation of recommended measures. Implementation is now under way. The measures vary in complexity and many require further evaluation by the industry or the authorities before implementation.

One of the measures completed in spring 2026 is new recommendations on individual payment preparedness which now include recommendations for points of sale. The recommendations are discussed in more detail in the article “Self-preparedness for payments”. A recurring theme is that both payers and payees should prepare to be able to use several different forms of payment.

Cash usage has declined but still plays an important role in the payment system, particularly for contingency purposes. Current digital

contingency arrangements are not sufficient to be able to reduce the contingency role of cash. The role of cash in the payment system is discussed in more detail in the article "Cash is still needed".

In Norway, bank deposits through bank transfers and card payments are currently the dominant means of payment, Both of these forms of payment can be made using a mobile phone, and mobile payments continue to increase. Mobile payments have long accounted for a dominant share of person-to-person (P2P) payments and now represent close to four out of ten payments at physical points of sale (see discussion below: "An efficient payment system"). This growth indicates that users find mobile payments both efficient and secure. However, in order to promote competition, cost efficiency and contingency preparedness, it is important that different payment cards and bank transfers are available as underlying payment solutions. The growing importance of mobile phones also suggests that the development of robust contingency arrangements for mobile payments if communication lines are disrupted should be prioritised.

Alongside changes in traditional payment methods, new payment systems with alternative means of payment are also being introduced. If these systems meet customer needs, establish sufficient trust and are perceived to offer attractive functionality, they may achieve broad adoption. Some of the new systems may reduce cross-border payment costs and processing times, while further expanding the role of global entities in the payment system. Stablecoins are an alternative payment channel that currently plays a negligible role in the Norwegian payment system. Stablecoins use open blockchains as transaction infrastructure. This creates opportunities, but both service development and further regulation are necessary to enable such infrastructure to be used as a general-purpose means of payment. Stablecoins have also not been sufficiently stable to function as a general-purpose means of payment. New regulation may mitigate price falls as a result of loss of confidence but does not address value fluctuations due to market frictions. The issue is discussed further in the article "Can stablecoins gain a foothold for general use?"

For a number of years, Norges Bank has assessed whether a central bank digital currency (CBDC) is needed to ensure that paying with the Norwegian krone will remain secure, efficient and attractive in the future. The conclusion is that introducing a CBDC is currently not warranted, but that the need may arise at a later stage. Norges Bank will continue to research tokenisation and different forms of CBDC in order to be able to introduce a CBDC should it become necessary for an efficient and secure payment system. The Bank will research the possibilities and consequences of tokenisation through activities such as technical and functional testing and in collaboration with other financial system entities. This work is discussed in more detail in "Tokenisation and central bank digital currency".

In focus

Self-preparedness for payments

Sound contingency arrangements among banks and other payment system participants are the first line of defence against disruptions and serious incidents affecting electronic payment services, but individual users also play a key role in limiting negative consequences. By following payment self-preparedness recommendations, both payers and payees contribute to payment system resilience.

Even though the payment system in Norway functions well, disruptions can occur, making services and functions that are taken as a given unavailable for shorter or longer periods. Such incidents can range from technical errors to extreme weather events and sabotage, and at worst military attacks.

By being prepared for an emergency, individuals primarily ensure that they and their immediate family are less affected by both small and large incidents. At the same time, this relieves the pressure on the payment system as a whole.

Self-preparedness for making payments

For several years, Norges Bank has published practical advice on payment self-preparedness, focusing on which payment alternatives the general public should have available:

- Multiple and different types of payment cards
- Some cash
- Accounts in multiple banks

Norges Bank's advice emphasises that it is important to have at least one physical BankAxept card since some of the current contingency arrangements for card payments are based on this type of card. It is also important that physical payment cards are regularly used with their chip (by inserting the card in a payment terminal) and entering the PIN. This ensures that the information stored on a payment card is updated, including any new preparedness functionality. Some international payment cards also have preparedness functionality that is activated when the card is used like this. Which functionality is available may vary between different types of cards and depends on the issuer.

Visit the websites of Norges Bank and the Norwegian Directorate for Civil Protection (DSB) for more practical advice on individual payment preparedness.

Self-preparedness for receipt of payments

In focus

To ensure that a payment is made, both payer and payee must have various payment alternatives available. Self-preparedness for receipt of payments is particularly important for points of sale that sell basic necessities.

In order to follow up recommended measures from a working group that has assessed contingence arrangements in the digital payment system on behalf of the Ministry of Finance, Norges Bank has coordinated a collaboration to draw up general preparedness guidelines for points of sale (see box). The collaboration has included representatives from Virke (the Federation of Norwegian Enterprise), NHO Service (Norwegian Federation of Service Industries and Retail Trade), NorgesGruppen (owner of grocery store chains), Coop Norge SA (the Norwegian consumer co-operative group), Rema 1000 (a Norwegian grocery chain) and Circle K (a multinational convenience retail chain). The recommendations are now published on norges-bank.no and individual firms are urged to adapt these recommendations to their own circumstances and specify measures.

Self-preparedness for payments at points of sale

The payment system in Norway is efficient and secure, and serious disruptions are rarely experienced at points of sale in Norway. Even though solutions are secure and business continuity arrangements are in place, problems may nevertheless arise. To ensure that points of sale can receive customer payments even during disruptions to regular payment solutions, Norges Bank recommends that points of sale consider the following self-preparedness measures:

Multiple card solutions: As a backup, when one specific card solution does not function, payment terminals should support multiple card solutions via both physical cards and mobile phone digital cards.

Payment terminal alternatives: Alternative payment channels provide a backup solution when customers cannot make terminal-based card payments. Examples include the generation of payment requests using QR codes and mobile apps.

Offline payments: Offline payments provide a backup solution when the payment terminal has no connection with the central payment infrastructure. Payments will be sent from the terminal once connection is re-established.

Backup cash register systems: Access to an independent backup solution for both cash register systems and payment terminals provides support when regular cash register systems do not work.

Cash: Cash payments provide backup when other payment solutions are unavailable, and consumers have a statutory right to pay with cash at points of sale. Both regular cash register systems and backup cash register systems must therefore support cash payments. Points of sale should also have some change available for both types of system.

General self-preparedness supports payment self-preparedness
In some scenarios, the effect of the aforementioned preparedness measures also depends on more general preparedness measures being in place. In line with general recommendations from the Norwegian Directorate for Civil Protection, the following contingency measures should also be considered:

Alternative lines of communication: Access to multiple lines of communication for cash register systems and payment terminals provides a point of sale with backup solutions if the primary line of communication is disrupted.

Emergency power supply: Although backup solutions for communication, cash register systems and payment terminals can be powered by batteries for a limited time, other functions may require an emergency power supply.

Rehearsed contingency plans: Well-functioning contingency solutions depend on points of sale staff knowing how to use them, and a regularly rehearsed contingency plan is an important tool in this regard.

Cash is still needed

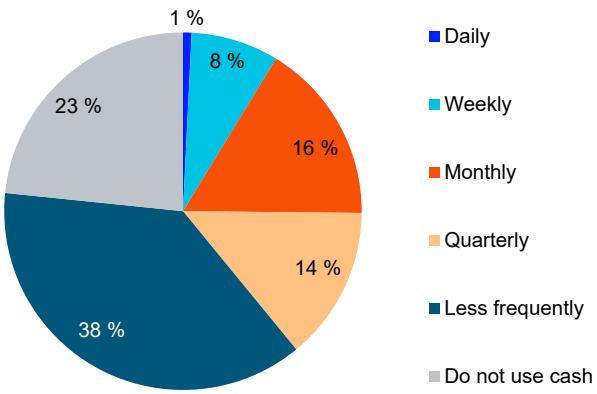
Norway is one of the countries with the lowest cash usage in the world. The vast majority of payments are made digitally, and a secure and efficient payment system is primarily ensured through robust digital solutions. Cash still plays an important role in the payment system. Cash is particularly important for contingency purposes and for individuals who do not have digital literacy or access. For cash to fulfil its functions, availability and ease of use is crucial.

The strengthening of the right of consumers to pay cash, which entered into force in 2024, and banks' statutory duty to provide their customers with adequate cash services are important contributions to ensuring this. At the same time, the provision of cash services is vulnerable and has certain weaknesses. If banks do not secure satisfactory solutions themselves, more detailed regulation should be drawn up.

The cash share of payments is low, but many people regularly use cash

Cash usage declined over a long period and fell further during the pandemic. Since 2020, the share of cash payments at physical points of sale and the share of P2P payments has been stable at around 3%.

Chart B.1 How often do you use cash?



Source: Norges Bank

For a more comprehensive picture of the use of and attitudes towards cash, Norges Bank conducted a somewhat more extensive survey targeted at private individuals in 2025 Q4.[1]

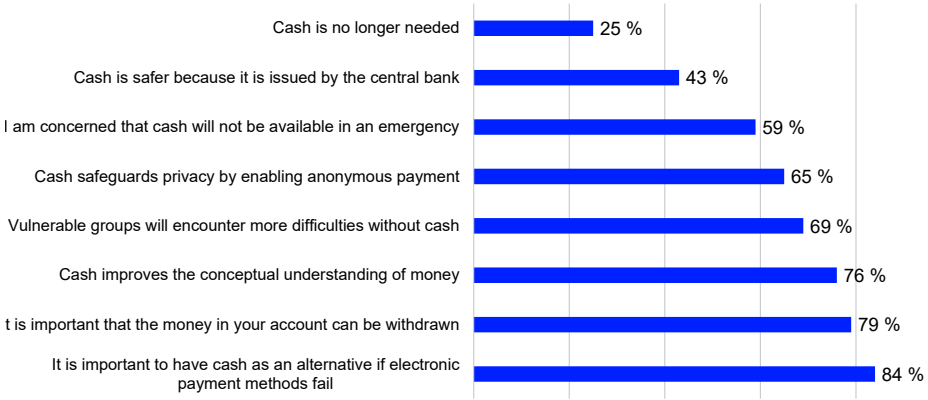
The survey shows that although the majority of the population rarely or never uses cash, a significant share nevertheless uses cash regularly. One in four uses cash at least once a month. Cash usage is more common among individuals with lower levels of education or lower income.

Just over 90% of cash users have access to online banking, payment cards and Vipps and use these solutions more frequently than they use cash. However, access to these payment methods is generally somewhat lower (4–5 percentage points) among cash users than in the population as a whole.

The survey shows that a large majority considers it important to have cash as an alternative if electronic payment methods fail. A majority also fully or mostly agrees that cash improves the conceptual understanding of money and that vulnerable groups will encounter more difficulties without cash. One quarter of respondents consider that there is no longer a need for cash.

36% of the population has cash available for everyday use, while 42% report that they have set aside cash for contingency purposes. The average cash holding among those who report having cash for everyday use is just under NOK 800, while the median value is NOK 500. For contingency holdings, the cash levels are higher. Among those respondents reporting that they have such cash reserves, the average holding is just above NOK 4 000, while the median value is NOK 2 000. A large majority of the population, 79%, consider that it is important to be

Chart B.2 To what extent do you agree with the following statements on the importance of cash availability?
Percentage responding “strongly agree” and “somewhat agree”



Source: Norges Bank

1 See Norges Bank (2026e). The survey focuses on the general population, including cash users. In the survey, a cash user is defined as someone who uses cash at least once a month.

able to withdraw and deposit cash, irrespective of their own use. Only 5% report that this is not important.

The 1000-krone banknote is still a valid means of payment

Norges Bank has undertaken a new assessment of the denomination structure and has decided that the 1000-krone banknote will remain a valid means of payment and can continue to be used like it is today. At the same time, it has been decided that banks can no longer order the notes from Norges Bank. The number of 1000-krone notes in circulation will thus gradually decline in the years ahead.

The reason for the assessment is that there have been substantial changes in the use of cash and the payment system since the previous assessment, which was conducted in connection with the introduction of the current banknote series. The Ministry of Finance also asked Norges Bank to make such an assessment, referring to Økokrim's (the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime) arguments for the withdrawal of the largest denomination, and the fact that cash usage has changed substantially over the past few years.[2]

In the assessment, Norges Bank has given weight to: the role of cash and its function in normal and contingency situations, efficient and secure cash handling and countering economic crime. The 1000-krone banknote currently accounts for a small share of total banknotes in circulation. In normal situations, cash therefore is of limited significance to cash payment efficiency. In severe contingency situations, however, there may be a need to distribute large volumes of cash over long distances and to make both more frequent and larger cash payments than normal. In such situations, the 1000-krone banknote may be important, and Norges Bank can put more of the 1000-krone banknote into circulation if necessary.

Regulatory limitations must be proportionate.

Cash has characteristics that make it suitable for use in certain forms of crime, including money laundering. This is one of the reasons why provisions in various regulatory frameworks have been introduced to set thresholds and other limits on the use of cash. Norges Bank recognises the need for such limitations. At the same time, measures must be proportionate. Both the regulatory framework and its enforcement must not undermine the role played by cash in contingency arrangements and financial inclusion, or public confidence in cash as a general-purpose and easy to use means of payment.

In the consultation on the transposition of the new EU anti-money laundering legislative package into Norwegian law, a lowering and

2 See letter from the Ministry of Finance to Norges Bank of 15 January 2026.

harmonisation of cash payment thresholds is proposed in the Anti-Money Laundering Act (currently NOK 40 000) and in the Financial Contracts Act (currently NOK 20 000). The proposed thresholds are NOK 20 000, or alternatively NOK 10000.[3]

Norges Bank considers that a reduction of the cash threshold in the anti-money laundering framework from NOK 40 000 to NOK 20 000 may be justified, given the considerations underlying the provision. It would then still be possible to carry out most purchases associated with daily life using cash, including goods that are purchased less frequently but are necessary in today's society. Norges Bank notes that there may be considerations suggesting the cash threshold for the right to pay cash under the Financial Contracts Act can be set somewhat lower, for example at NOK 10 000 or NOK 15 000. Consumers would then still have the right to pay cash for most necessary everyday purchases. Combined with a cash threshold under the Anti-Money Laundering Act of NOK 20 000, this could provide sufficient flexibility to safeguard financial inclusion and contingency preparedness.

Norges Bank also points out that a cash threshold below NOK 20 000 entails a considerable restriction on contractual freedom and on the ability of consumers and retailers of goods and services to use cash as a means of settlement. Norges Bank questions whether a harmonised threshold of NOK 10 000 would be in line with the proportionality requirement and is of the opinion that a cash threshold as low as 5 000 would not be justified.

A reduction in cash payment thresholds does not itself imply a reduction in what may be regarded as adequate cash services.

Banks are responsible for providing adequate cash services

Section 16-4 of the Financial Institutions Act stipulates: "Banks shall, in accordance with customer expectations and needs, accept cash from customers and make deposits available to customers in the form of cash". This obligation means that private individuals are to have sufficient opportunity to withdraw and deposit cash, and that businesses must be able to access change and deposit cash revenue. This assumes that there is both sufficient geographical coverage and other necessary functionality. Banks can fulfil this obligation themselves or through agreements with other cash service providers.

Norges Bank has previously pointed out that the current provision of cash services is vulnerable and has certain weaknesses. Most cash handling processes and cash services are carried out by entities that are not legally obligated to do so. Over time, the number of bank branches offering over-the-counter cash services has steadily declined, as has the

3 Høring – arbeidsgrupperapport om EUs antihvitvaskingspakke [Consultation – Report from the working group on the EUs anti-money laundering legislative package] – regjeringen.no (in Norwegian only):

number of ATMs. In-store cash services (KiB), a service for cash deposit and withdrawal available in approximately 1450 of NorgesGruppen's grocery stores, now account for a substantial portion of banks' cash services. KiB services are largely adequate for most consumers but are only available to BankAxept cardholders. It also fails to cover the business sector's need to make large cash deposits and access change.

Banks' obligation to provide cash services also applies in situations when demand for cash rises, for example if electronic payment systems are disrupted. In terms of contingency preparedness, it is a weakness that KiB services do not function when the BankAxept backup solution[4] is in use. This means that a large share of banks' cash supply is cut off when payment terminals are offline and therefore that the general public's opportunity to withdraw cash is then substantially reduced.

The general wording of current regulations may make it difficult to define "sufficient cash services". Nevertheless, it would be preferable if banks, without more detailed regulation, were to collectively secure satisfactory coverage of cash services across Norway. However, Norges Bank emphasises that banks' responsibility to supply cash applies regardless of a well-functioning service provider market. If banks do not secure satisfactory solutions themselves, more detailed regulation should be drawn up. The previous mapping of the provision of cash services in Norway was carried out in 2020/2021. A new survey of cash services is now needed.

4 An electronic backup solution that is activated, for example, in the event of point of sale communication outages.

Tokenisation and central bank digital currency

Norges Bank is exploring? whether introducing a central bank digital currency (CBDC) is necessary to ensure that the Norwegian krone will be a secure, efficient and attractive means of payment in the future. Towards the end of 2025, Norges Bank concluded that the introduction of a CBDC in Norway was not warranted for the time being. However, needs may change and the exploration is continuing so that Norges Bank can be ready to introduce a CBDC if this becomes necessary to ensure an efficient and secure payment system. For example, a need could arise for facilitating settlement in central bank money of interbank transactions in tokenised assets. Use of tokenisation is limited in Norway compared with some other countries, but developments could quickly accelerate. Norwegian banks should actively monitor the development of this technology. Norges Bank has extended its collaboration with financial market participants in the further exploration of potential benefits and challenges of the technology and will also involve banks in technical testing of tokenisation and CBDCs.

Central bank digital currency

CBDC is electronic money issued by the central bank in the official unit of account. There are two main variants of CBDC: retail and wholesale. A retail CBDC will be generally available to the public on par with cash and bank deposits and should be possible to use at retail level, for example at points of sale, between private individuals and for online purchases.

A wholesale CBDC is tokenised central bank reserves and would only be available to banks and other institutions in the financial sector that have an account at the central bank. It could be used for settlement of interbank payments etc. in the same way that central bank reserves are used in the current interbank system but in a different technological form. This type of CBDC may be necessary for ensuring that settlement of transactions involving tokenised bank deposits or related to transactions with tokenised securities are conducted effectively and without unacceptable risk. Tokenisation is discussed in further detail below.

Norges Bank does not currently recommend the introduction of a CBDC

Norges Bank is exploring whether introducing a CBDC is necessary for ensuring that the Norwegian krone will remain a secure, efficient and attractive means of payment in the future.

Today, the Norwegian payment system is efficient and secure. Operations are reliable and payments can be made swiftly at low economic cost and in ways that are adapted to users' needs. Contingency arrangements in the payment system are sound and efforts are being made to strengthen them further. The use of tokenisation technology has not progressed very far in the Norwegian financial industry.

This is why Norges Bank, towards the end of 2025, concluded that the introduction of a CBDC in Norway was not warranted for the time being.[1] However, the need for a CBDC in Norway may change. The technology in the financial system is advancing rapidly, and new services and participants are emerging. Hence, the need for such a currency may change in the future. Therefore, Norges Bank will be ready to introduce a CBDC at a later date, if it becomes necessary in order to maintain an efficient and secure payment system. Norges Bank is therefore continuing its CBDC and tokenisation research.

Retail CBDCs are uncommon

Only a few central banks have issued a CBDC. The central banks of Nigeria, Jamaica and the Bahamas have issued retail CBDCs, partly to promote financial inclusion and reduce cash distribution costs. However, the usage is relatively limited so far. Further, rhe central bank of China has issued a CBDC in a pilot with many users. Usage in China is reported to have picked up after the introduction of interest on CBDC holdings. Central banks in many countries comparable to Norway have concluded, for the time being, that the issuance of a retail CBDC is not warranted.

The European Central Bank (ECB) is probably the advanced economy central bank that has made the most progress in its preparation for issuing a retail CBDC – a digital euro. One of the arguments for a digital euro is that Europeans will then gain access to a payment system that is not reliant on payment service providers based outside of Europe. Consequently, a digital euro would enhance Europe's strategic autonomy in a period of heightened geopolitical uncertainty.[2] An introductio of a digital euro depends on amendments in EU legislation. The ECB will make a final decision on the introduction of a digital euro once the statutory basis has been established. The ECB states that if necessary, regulation is adopted in the EU in 2026, a digital euro can be introduced in 2029.

1 See Norges Bank (2025b) and Norges Bank (2026a).
2 See for example Cipollone (2026) and Norges Bank (2026b) for an overview of the digital euro project.

The ECB/euro system has also explored and tested central bank money settlement solutions for transactions and trades in tokenised assets. In this connection, the ECB has published a plan where the first stage is to amend the current settlement system for euro (T2) so that transactions in tokenised assets can be settled in central bank money in T2. This is scheduled to be in place at the end of Q3 2026.

In the longer term, the ECB is exploring the benefits and challenges of establishing a separate blockchain-based platform for settlement of tokenised transactions in central bank money. Whether and when such a solution will be introduced is still uncertain.

Tokenisation – characteristics and applications

Tokenisation is a process in which an asset is represented as a digital unit – a token – on a ledger based on blockchain or distributed ledger technology (DLT).[3] Tokens and DLT are best known from cryptocurrencies, but the technology can also be used to record and transfer ownership to other assets such as securities, bank deposits, real estate and central bank money. Before this can happen, the assets must be "tokenised" and recorded on a blockchain so that transactions can be conducted digitally and be traceable. Tokens can be a digital mirror image of an existing asset or be issued as a new asset on a blockchain.

The use of tokenisation is still rather limited in the traditional payment system and financial industry. To date, blockchain technology has mainly been used outside of traditional finance. The technology has particularly been used as a basis for cryptocurrencies, partly with the intention to establish an ecosystem or infrastructure that is independent of any central entity, such as banks, central banks or other firms or government authorities. In some cases, the motivation may be that such transfers are subject to less regulation, control and insight from public authorities than regular transfers. Such motives do not of course apply if a central bank decides to participate in the establishment of tokenised financial infrastructures.

One of the most important benefits of tokenised assets and blockchain technology is programmability through the use of smart contracts. Smart contracts are computer programs that perform automated transactions when predefined conditions are met. Automation can reduce the need for intermediaries and enhance the efficiency of processes such as securities trading and FX transactions.

Smart contracts can also facilitate atomic settlement, which means that a transaction is only completed if, and only if, all parties fulfil their obligations and where the ownership transfer of all elements in the transaction takes place concurrently and immediately. This can be a

3 See Cipollone (2026). A blockchain is a distributed ledger or decentralised data system. The units in the ledger are accessible through cryptographic codes.

robust and efficient way of achieving delivery versus payment and payment versus payment. Such characteristics remove counterparty and settlement risk when settling trades involving for example securities and foreign currency.

The programmability and other characteristics of blockchain technology may give stablecoins an advantage in some new payment areas. A number of stablecoin providers are aiming to play a larger role in traditional payments and finance (see the article "Can stablecoins gain a foothold for general use?"). At the same time, market participants in traditional finance in some countries have started testing trading in tokenised securities, using stablecoins as a means of settlement. Central banks emphasise that the means of payment in such trades should be central bank money because alternatives such as stablecoins and other private means of settlement may entail a certain amount of risk.

Tokenisation can provide new opportunities

What are the advantages of using tokenisation and blockchain technology in the payment system and financial industry? Does this technology have characteristics that preclude realising the same benefits through the improvement of current payment solutions and technology?

Many central banks, financial institutions and international organisations are carrying out tests and analyses to answer these questions. Some central banks are pilot testing business models, for example with existent securities and money. The majority of the testing is based on the design of existing payment functions and services, such as in connection with cross-border payments and securities settlement. However, it may be that the substantial gains will be achieved because the technology provides entirely new and more efficient ways of performing basic services, which entail a number of gains that are currently unknown.

Technological restructuring can be extensive and will be more demanding the higher the number of institutions and functions that have to be changed to realise the gains. This suggests that an extensive restructuring towards tokenisation is only warranted if it enables the development of new and far more efficient payment services. Minor improvements to existing services will, however, not be sufficient to warrant extensive restructuring. It will likely only be possible to verify the largest gains from the technology once it has matured and developments have progressed substantially further. Such gains may materialise if payment functions are linked to other functions, so that the overall user experience and benefits are enhanced and the number of parties and systems involved in a transaction is reduced.

Further exploration of tokenisation and CBDC

In focus

Norges Bank will continue to explore tokenisation and CBDC to be prepared to introduce a CBDC at a later date if it becomes necessary. The Bank will therefore monitor the development of tokenisation, both internationally and in the Norwegian financial sector. Realising potential benefits from tokenisation will require restructuring several elements in the financial ecosystem, which will impact many stakeholders. Potential benefits and costs of tokenisation will largely be realised outside the central bank and as a result of a coordinated technological shift among a number of market participants. Consequently, the central bank would benefit little from being the sole parti in the financial infrastructure to introduce tokenised solutions. Going forward, Norges Bank will therefore emphasise involvement and collaboration with other banks and payment system participants. Norges Bank will continue with technical and functional testing of various test cases in our technological sandboxes, and has invited ther banks and financial sector participants to take part in the testing.[4]

The Norwegian financial industry has a long and proud tradition of leading the way in the development of efficient payment services and implementation of new technology in the financial infrastructure. Progress has been made from working together on a shared infrastructure that facilitates competition on payment services. Such coordination may also be necessary for realising the gains of tokenisation.

The limited use of tokenisation so far may be partly due to an unclear balance of risks. Access to a means of settlement in which the market has confidence, such as central bank reserves, could be an important factor in the development of tokenisation and smart contracts in the financial system. At the same time, there may be a risk related to the issuing of and registration of assets on blockchains given the underlying technology. Furthermore, there are still unresolved legal issues related to whether ownership of a token on the blockchain also provides indisputable ownership of the asset itself. Such issues must be resolved in order for transactions involving tokenised assets to become widely adopted in the regulated part of the financial system. International standards in this field may be implemented due to market developments and/or regulation.

Norges Bank is currently in formal discussions with the ECB about participation in the Eurosystem's settlement system T2. Participation in the Eurosystem's solutions for a CBDC and other settlement methods in central bank money for transactions in tokenised assets may be relevant at a later stage if Norges Bank enters into an agreement to participate in T2.

4 So far, Norges Bank's testing of technical solutions has been discussed in Norges Bank (2026c) and Norges Bank (2023).

Can stablecoins gain a foothold for general use?

Stablecoins are predominantly used in cryptoasset investment, but some other applications are emerging. Stablecoins have attracted considerable attention for their potential benefits in the payment system and their potential risks. A number of countries have introduced regulations. In Norway, EU regulations have been transposed into the Crypto Asset Act. The regulations mitigate many of the risks associated with stablecoins but are currently insufficient to enable stablecoins to become stable general-purpose means of payment.

Stablecoins are mainly used for cryptoasset trading, but new applications are being tested

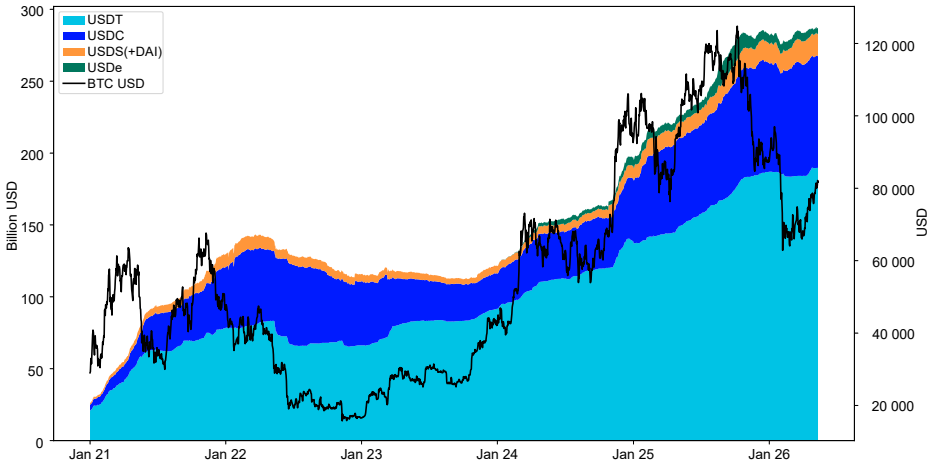
Stablecoins are cryptoassets designed to maintain a stable value against a reference asset, and 99% of the total market value of stablecoins, around USD 300bn, is pegged to the US dollar. The US administration has promoted stablecoins as an instrument to preserve and strengthen the international role of the US dollar and ensure demand for US government securities. The market for euro-denominated stablecoins amounts to around EUR 0.5bn.

The applications for stablecoins have mainly been linked to cryptoasset speculation. Stablecoins are used both as a means of settlement and as a store of value, including investment in various interest-bearing services. Historically, the total value of stablecoins has fluctuated in line with cryptoasset market developments (Chart C.1). Recently, the stablecoin market has continued to grow while the value of bitcoin and many other cryptoassets has fallen, indicating the emergence of new applications. Many market participants have predicted significant stablecoin growth ahead, also in new applications.[1]

However, predicting the use and value of these new applications is not simple. McKinsey and Artemis Analytics (2026) point out that the transaction volume for stablecoins on blockchains exceeds USD 35tn per year, but that most is unrelated to ordinary payments and money transfers. Their analysis finds that such payments only amount to USD

1 IMF (2025) p. 27.

Chart C.1 Market value of the largest stablecoins (lhs) and bitcoin price (rhs))



Source: Coingecko

390bn, around 0.02% of traditional payments globally. The largest share of stablecoin payments is between private individuals, including cross-border payments. Some other types of stablecoin payments, such as between firms, represent a lower but faster-growing share.

One barrier to general usage is that stablecoins are issued by market participants that are not widely known to the public and unavailable through the interfaces normally used by customers for ordinary payments. This may now be changing. New regulations that set out user rights and requirements for issuers may increase confidence in stablecoins in general. This confidence will likely be even stronger if stablecoins are issued or provided by market participants users already trust. In autumn 2025, it became known that nine European banks are planning the joint issue of a euro-denominated stablecoin, and more banks have later joined. It also became known that payment service provider Klarna is planning to issue a stablecoin.

Stablecoins play a negligible role in the Norwegian payment system. In 2024 and 2026, Norges Bank carried out surveys about cryptoasset use and awareness.[2] Both surveys showed that stablecoin use and awareness was limited. The 2026 survey showed that 19% of the Norwegian population[3] had heard of stablecoins and that 72% of that group had never used them. The three main reasons given for buying stablecoins were: trading with another cryptocurrency (55%), using as a store of value (30%) and learning more about and/or testing the technology (22%).

2 Norges Bank (2024) and Norges Bank (2026d). The surveys covered individuals, not institutions and firms.
3 16 years or older.

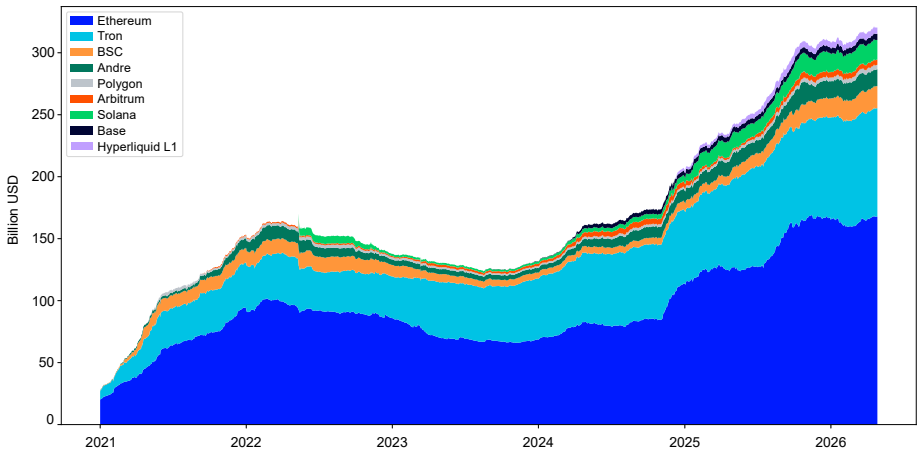
Open blockchains make stablecoins accessible, but they also present some challenges

Stablecoins use open blockchains as their basic transaction infrastructure, with the advantage that they, like other cryptoassets, can be transferred around the clock on all days of the week without any central intermediary. The Ethereum blockchain accounts for the largest share of stablecoin value, but other blockchains also account for a substantial share. In addition, there are second-layer solutions that run on top of other blockchains and direct transactions elsewhere to avoid congestion on the blockchain itself (Chart C.2).

One issue in connection with the use of open blockchains for stablecoin transactions is that transaction fees must be paid in the cryptoasset associated with the blockchain in question. Using e.g. Ethereum as the transaction infrastructure means that fees will have to be paid in the cryptoasset Ether. These fees contribute to rewarding those that participate in the consensus mechanism to update the blockchain. This means that users must hold these cryptoassets to carry out transactions, and the costs can become unpredictable and high, in particular if the blockchain is operating close to capacity. However, this has become less of a problem with new scaling solutions. Some stablecoin issuers, such as Circle, develop their own blockchains where fees can be paid in stablecoins. This reduces dependency on free-floating cryptoassets when carrying out transactions but may also amplify monopolistic tendencies by increasing the network advantages of some stablecoins.

Stablecoins function as bearer instruments linked to cryptographic codes and can be transferred to anyone without requiring a customer relationship with the stablecoin issuer in advance. This makes them more accessible compared with other electronic money but also carries some disadvantages. Should cryptographic codes be lost or made available to

Chart C.2 Stablecoin market value across different blockchains



Source: DeFiLama

unauthorised parties through cybercrime, the money can be lost. BIS (2025b) points out that stablecoins lack the necessary know-your-customer and transaction controls that safeguard the integrity of the traditional payment system.

A number of services are being developed that may facilitate stablecoin use. Third parties can shield users from the underlying technology and relieve customers of the need to relate to blockchains. For example, various payment applications offer payment using stablecoins, where the stablecoins appear in the user's account and can be used like e-money or bank money. In such cases, the payment applications often manage the cryptographic codes. Payments between customers will often only be carried out as payments between accounts in the payment providers' internal accounting system, with no changes in the blockchain. Changes in the blockchain will only be made if customers want to withdraw the stablecoins from the internal accounting system. Although this may simplify matters for customers, they will also incur a counterparty risk as a result of their exposure to these providers.

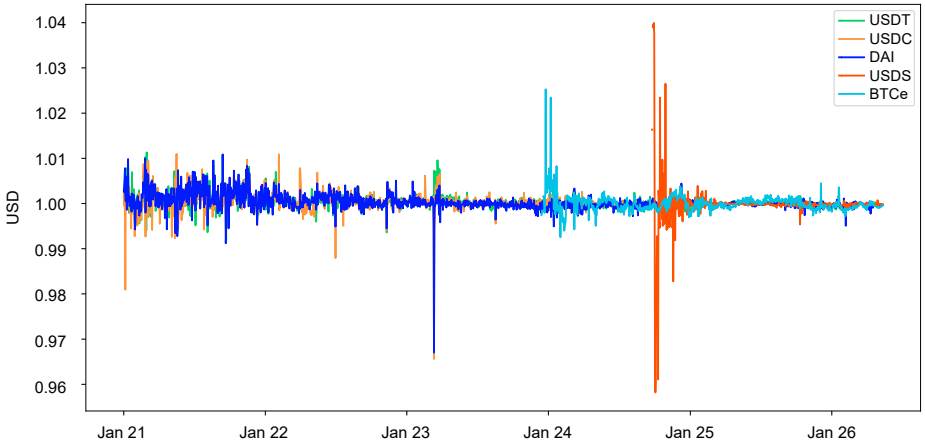
There are also market participants that develop underlying payment channels based on stablecoins without the users having to relate. For example, a payer and a payee can carry out an international transaction where payment is made from the payer's bank account to the payee's bank account with underlying settlement in stablecoins. The large card companies are also developing payment solutions with stablecoins as the underlying payment infrastructure.

Using open blockchains as financial infrastructures presents a number of challenges. For instance, decentralisation could present challenges related to the management and control required for financial infrastructures. This could require other types of regulation and obligations for service providers and users. In traditional financial infrastructure, there are clear risk distribution regulations and compliance responsibilities. These regulations cannot be applied directly when open blockchains are used as transaction infrastructure. Should stablecoins become more widespread, there will be a need to further develop regulations governing stablecoin payments.

Regulations cannot easily make stablecoins stable

BIS (2025b) points out that instability and an inelastic money supply prevent stablecoins from functioning as an alternative means of payment. The stability and singleness of all forms of money in the same currency is a crucial key characteristic of money, meaning that users do not have to use resources to determine the value of the money itself and that different recipients can put the same value on the means of payment. Users may accept minor value fluctuations for individual, low-value transactions, as long as usage provides other cost savings and benefits.

Chart C.3 Fluctuations in stablecoin values intended to be stable against USD



Source: Coingecko

However, value fluctuations will be problematic for a general-purpose means of payment that is also used for larger payments. Chart C.3 shows that even the largest stablecoins on the market have been subject to value fluctuations, resulting in both uncertain values for individual stablecoins and differing values relative to each other.

Value fluctuations, in particular falls in value, can be due to loss of confidence in the stablecoin issuer's reserves. One example of this is the fall in value of USDC when the Silicon Valley Bank collapsed in March 2023 because Circle's reserves were partly held in the bank. Should users lose confidence that a stablecoin will maintain its value, a mass sell-off could push the value further down. This may also result in a run on redemptions, causing assets that back the value of the stablecoin to fall in value. This could spill over to other parts of the financial sector and threaten financial stability. The economic scope of stablecoins and the exposure of traditional financial institutions are currently likely too limited for such falls in value to threaten financial stability. This may change.

Confidence in the value can be strengthened through regulation. Quality requirements for securities that back the stablecoin will strengthen confidence. Stablecoin backing requirements are key in the European Markets in Crypto-Assets Regulation – MiCAR – which was also transposed into Norwegian law from 1 July 2025 with the Cryptoassets Act. Such requirements are also key in the new US stablecoin legislation – the GENIUS Act.

Should stablecoins become large enough, it may become difficult to ensure confidence even if reserve assets comprise the safest securities. The academic literature shows that stablecoin issuers' share of US short-term government debt is already large enough for issuance and redemptions to influence the price and therefore the yield on these

securities.[4] The Bank of England has proposed[5] that systemically important issuers of sterling-denominated stablecoins should be partially secured with access to a deposit account at the Bank and access to a backstop lending facility to ensure confidence in stablecoins. Norges Bank is not aware of similar proposals from other central banks.

Value fluctuations can also be caused by supply and demand imbalances. Flexible issuance of stablecoins by providing loans on demand, as is the case for bank money, is not possible, and stablecoins are not interoperable in the form of central bank money settlement as is the case for bank money. Each issued stablecoin must be backed in advance and it can take time to redeem stablecoins for bank money. While stablecoins are used and traded 24/7, the markets for the securities that form part of the reserve assets will have limited operating hours. Settlement may also take some time.

Issuing new stablecoins and taking existing stablecoins out of circulation is therefore not frictionless. If for example, there is surplus demand for a stablecoin, the price may exceed face value. As each individual stablecoin is a closed system for each individual issuer with its own supply and demand, stablecoins will fluctuate in value in relation to each other. Value fluctuations resulting from supply and demand mismatch can be amplified by an issuer often having issued a stablecoin across different blockchains with different liquidities. This may entail not only that a stablecoin fluctuates in value, but that it is traded at different prices on different blockchains.

Requirements to hold assets backing stablecoins in advance may increase the friction around issuance and destruction. Thus, requirements set to prevent a fall in value resulting from loss of confidence may increase value fluctuations due to supply and demand imbalances.

Tokenised bank money is backed by a comprehensive regulatory and institutional framework and may provide a more stable tokenised money alternative to stablecoins. Payments in tokenised bank money should be settled in central bank money. Developments in the tokenisation of money and other assets and settlement in central bank money is discussed in more detail in the article "Tokenisation and central bank digital currency".

4 Ahmed & Aldasoro (2026).
5 Bank of England (2025).

Quantum computing threats and financial system measures

Quantum computing represents a threat to the security of current IT systems. To address this, efforts are under way at national and international levels to implement post-quantum cryptography (PQC). Organisations both within and outside the financial system should prioritise the measures needed to maintain the security of their IT systems.

Why does quantum computing pose a threat to IT security?

Quantum computing uses principles from quantum physics to perform certain computations more efficiently than classical computers, enabling new applications while also introducing potential security risks.

Most networks in the financial system are completely dependent on cryptography to ensure confidentiality, integrity and authenticity. Fundamental security protocols are based on cryptographic algorithms that have been considered secure for decades. However, advances in quantum computing challenge these underlying security assumptions in important respects.[1] Quantum computing has advanced to the point where attacks enabled by quantum capabilities are considered *likely*.

The consequences may be substantial. Security authorities in Norway and other countries[2] have therefore recommended and in some cases required the issue to be addressed before it becomes critical. Some of them assume a transition to PQC algorithms by 2035, while others are aiming for a faster introduction.

Solutions exist and more are in the pipeline

PQC consists of cryptographic algorithms designed to withstand attacks from both quantum and conventional computing.[3] They do not require any form of quantum technology to be implemented and are intended to function within existing infrastructure.

1 Integer factorisation and discrete logarithms using Shor's algorithm.
2 Inter alia NSM, ENISA, NIST, BSI, ANSSI and NCSC.
3 See NIST CSRC PQC (2024).

It should be noted that not all forms of cryptography are vulnerable to quantum attacks.[4] The threat is particularly linked to two components of cryptographic protocols:

- *Key exchange* that is used to establish a shared secret key between parties (e.g. between a client and a server).
- *Digital signatures* that are used to authenticate interacting parties.

In both cases, new PQC alternatives[5] are available and will cover many use cases.

However, more alternatives[6] may emerge and it is therefore necessary to determine which solutions are appropriate in different use scenarios. In any event, the general recommendation is to use standardised algorithms.

Some challenges

The financial system is vast and complex, and there might be subsystems that lack the flexibility to use the new building blocks directly. As recommendations to plan for the implementation of PQC algorithms are already in place, it is important to ensure that future systems are capable of adopting them.

The transition may take time if there are system-related technical complications. For example, PQC signatures are considerably larger than conventional signatures, and this may increase the overall use of resources. This will be addressed over time but may pose challenges where standard formats[7] or hardware[8] need to be upgraded. In some cases, products intended to handle new standards will also need certification, potentially extending the transition period further.

Who is responsible for PQC?

Individual entities in the financial system are responsible for securing their own systems. This includes banks, other financial institutions and owners of systems within the financial infrastructure. This responsibility applies to all forms of IT security, including PQC.

Cyberattacks that disrupt critical functions or lead to a broad loss of confidence may threaten financial stability. This provides a rationale for measures through industry organisations and authorities.

Finance Norway has developed a roadmap for managing quantum risk in the Norwegian financial sector.[9] The roadmap provides a common,

4 Certain forms of symmetric cryptography such as block ciphers or cryptographic hash functions are not materially vulnerable to quantum attacks.

5 See NIST CSRC PQC (2024).

6 NIST, ISO and other bodies may ultimately use alternative algorithms.

7 ISO 8583 is an example.

8 For example, tris may relate to chips in payment cards or HSMs (Hardware Security Modules – hardware used to implement cryptographic functions) that are designed for older algorithms.

9 See Finance Norway (2026).

structured and risk-based framework for the PQC transition and recommends that financial sector entities implement such solutions by 2035. On June 7 2026,

NSM is responsible for providing guidance in the transition to new algorithms, and guidance material has also been published to assist in planning and execution.[10] NSM published a position paper encouraging all organizations to address the quantum threat by 2030.[11]

Finanstilsynet (Financial Supervisory Authority of Norway) follows up the management of quantum risk in the financial system by supervising individual financial sector entities. The topic is also addressed in Finanstilsynet's annual *Risk and Vulnerability Analysis* report.[12]

Norges Bank follows up PQC in its own systems and will do so in its supervision of interbank systems and in its broader oversight of the payment system.

What is happening at the international level?

In January 2026, the G7 Cyber Expert Group (CEG)[13] published joint strategic recommendations for the transition to PQC.[14] These include early identification of cryptographic dependencies, testing of PQC algorithms and strengthened cooperation between banks, infrastructures and vendors, with particular emphasis on risks associated with long-lived data and third-party dependencies.

In parallel, the BIS Innovation Hub[15] is facilitating practical experimentation through Project Leap.[16] The project has demonstrated, together with European central banks and SWIFT, that traditional digital signatures can be replaced with PQC in actual payment messages, and that hybrid encryption schemes can support secure transitions from existing systems. These experiences also highlight some of the challenges involved: Since signatures and keys may be large, there may not be sufficient space in standardised message formats, and processing time for each transaction may increase significantly.

Work in international fora has direct implications for Norwegian entities. The SWIFT infrastructure is key to both European and Norwegian payment systems, and through EEA obligations and regulatory frameworks such as DORA, Norwegian institutions will be subject to European requirements for cryptographic resilience and IT risk management.

10 See NSM (2023).

11 Posisjonsnotat om kvantenøkkeldistribusjon – Nasjonal sikkerhetsmyndighet (in Norwegian only).

12 See Finanstilsynet (2026).

13 This is a working group with representatives from financial authorities in the G7 countries and the EU, which coordinates policy and shares cybersecurity information.

14 See G7 CEG (2026).

15 BIS Innovation Hub is seeking to promote cooperation among central banks on innovative financial technology. BIS Innovation Hub has centres across the globe, including a Nordic centre in Stockholm

16 See BIS (2025a).

The path forward

The transition to PQC is among the most significant security changes envisaged in electronic systems. Unlike many earlier cryptographic problems that often had to be addressed at short notice, this transition is planned and gradual.[17] Important progress has already been made, but the work is far from complete. Early testing and integration of PQC solutions help ensure that current systems remain secure – even in the face of the advancing quantum threat.

Ensuring a timely transition is important for the security of the payment and financial systems. The transition to PQC must be prepared and implemented across the sector and in cooperation with the parties on which system function depends.[18]

In many cases, managing the transition to PQC is relatively straightforward: it involves deploying new or updated products from suppliers when they become available. In other cases, new standards must be established. Suppliers of critical components are following different timelines in adapting their products, and completion may take time. There may also be specific situations where additional measures are required. All of this must be addressed sooner rather than later.

Individual entities are responsible for securing their own systems. At the same time, it is important that the process in the financial sector proceeds in an orderly manner and ensures that the system end up with common functionality in line with the target state.[19] Entities that use cryptography must agree on what to use and when, otherwise the networks will not function as intended. Coordination is therefore needed to ensure that the transition is implemented in a sound manner.

17 However, the time available to complete the transition is limited, given that many systems will need to be updated.

18 Dependencies may be extensive: Supplier industry, supporting networks etc.

19 A PQC system should also be designed with sufficient adaptability to allow the replacement of algorithms if they become compromised.

Annexes

Tables[1]

Table 1 Average daily turnover in clearing and settlement systems (transactions)

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NICS											
NICS Gross	772	980	1 021	1 567	1 859	2 028	2 278	2 483	2 419	2 458	956
NICS Net (million)	9,1	9,5	9,9	10,5	11,1	10,1	9,7	10,0	10,0	9,7	9,6
NICS Real[1]						333 255	510 180	583 183	588 816	582 349	575 228
NBO											
Total number of transactions	1 565	1 835	1 958	2 555	2 745	2 935	3 175	3 540	3 782	4 595	13 577
RTGS Gross transactions excl. NICS	658	700	793	841	859	930	828	898	1 182	1 924	12 420

[1] The daily average for NICS Real is calculated using the number of calendar days.

Numbers for NICS are from Bits. Numbers for NBO are from Norges Bank.

Table 2 Average daily turnover in clearing and settlement systems (in billions of NOK)

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NICS	**285.9**	**284.1**	**297.0**	**315.3**	**323.2**	**347.0**	**351.7**	**408.7**	**417.5**	**404.8**	**259.9**
NICS Gross	160.1	158.7	163.3	175.2	176.0	196.1	189.3	232.4	236.2	219.4	73.7
NICS Net	125.8	125.4	133.7	140.1	147.2	150.6	162.0	175.8	180.9	185.0	185.8
NICS Real[1]						0.2	0.4	0.4	0.4	0.4	0.4
NBO	**219.3**	**221.2**	**235.8**	**247.6**	**259.3**	**458.1**	**327.4**	**338.6**	**355.0**	**350.0**	**359.0**
NICS Gross	157.5	156.1	159.0	172.2	158.0	178.5	169.7	203.0	204.9	204.1	71.5
RTGS Gross transactions excl. NICS	46.0	40.4	42.1	57.3	81.7	261.5	136.8	114.0	123.5	119.0	263.6
NICS Net	11.9	12.4	13.1	13.3	13.5	13.4	14.6	12.1	15.8	19.0	15.4
NICS Real[1]						0.0	0.0	0.0	0.0	0.0	0.0
VPO	3.8	3.7	4.2	4.8	6.0	4.7	6.2	9.5	10.8	9.7	8.4

[1] The daily average for NICS Real is calculated using the number of calendar days.

Numbers for NICS are from Bits. Numbers for NBO are from Norges Bank.

1 Tables showing developments in retail payment services are published in Retail Payment Services 2025.

Table 3 Number of participants in clearing and settlement systems (at year-end)

	2020	2021	2022	2023	2024	2025
Norges Bank's settlement system (NBO): Banks with an account in Norges Bank	122	118	118	111	104	95
Norges Bank's settlement system (NBO): Banks with retail net settlement in Norges Bank	21	21	21	20	19	19
DNB	87	86	83	82	76	66
SpareBank 1 SMN	10	9	8	7	6	6
Norwegian Interbank Clearing System (NICS)	119	118	114	111	103	95

Source: Bits and Norges Bank

Norges Bank's responsibilities

Norges Bank is tasked with promoting financial stability and an efficient and secure payment system.[1] In this context, the payment system comprises any means, systems or instruments that can be used to execute or facilitate payment transactions, with cash, deposit money and other means of payment. This is a broader definition than the definition in the Payment Systems Act (see box).

Norges Bank fulfils its responsibilities by, among other things:

- Providing for a stable and efficient system for payment, clearing and settlement between entities with accounts at Norges Bank.
- Issuing banknotes and coins and ensuring their efficient functioning as a means of payment.
- Overseeing the payment system and other financial infrastructure and contributing to contingency arrangements.
- Supervising interbank systems.

As operator, Norges Bank ensures efficient and secure operating platforms and sets the terms for the services the Bank provides. As supervisory authority, Norges Bank sets requirements for licensed interbank systems. Through its oversight work, Norges Bank urges participants to follow principles and standards for best practice and to

1 See Section 1-2 of the Central Bank Act and Section 2-1 of the Payment Systems Act.

Financial infrastructure

Financial infrastructure can be defined as a network of systems, called financial market infrastructures (FMIs), that enables users to perform financial transactions. The infrastructure must ensure that cash payments and transactions in financial instruments are recorded, cleared and settled and that information on the size of holdings is stored.

The financial infrastructure consists of the payment system, the securities settlement system, central securities depositories (CSDs), central counterparties (CCPs) and trade repositories.

Virtually all financial transactions require the use of the financial infrastructure. Thus, the financial infrastructure plays a key role in ensuring financial stability. The costs to society of a disruption in the financial infrastructure may be considerably higher than the FMIs' private costs. The financial infrastructure is therefore subject to regulation, supervision and oversight by the authorities.

make changes that contribute to maintaining an efficient and secure financial infrastructure. An efficient payment system carries out payment transactions swiftly, at low cost and adapted to users' needs.

Norges Bank's use of instruments in different areas will vary over time and be adapted to developments in the payment system and the financial infrastructure. Norges Bank is tasked with advising the Ministry of Finance when measures should be implemented by bodies other than the Bank in order to fulfil the purpose of central banking activities.

Norges Bank's approach to financial market infrastructure supervision and oversight

Norges Bank is the licensing and supervisory authority for the part of the payment system called interbank systems (Table 1). These are systems for clearing and settling transactions between credit institutions. If a licensed interbank system is not configured in accordance with the Payment Systems Act or the licence terms, Norges Bank will require that the interbank system owner rectify the situation. The purpose is to ensure that interbank systems are organised to promote financial stability. Norges Bank may grant exemptions from the licensing requirement for interbank systems considered to have no significant effect on financial stability.

Oversight entails monitoring FMIs and developments and driving improvements. This work enables Norges Bank to recommend changes that can make the payment system and other FMIs more secure and efficient. Norges Bank oversees the payment system as a whole and key FMIs are subject to permanent and regular oversight (Table 1).

TABLE 1 FMIs subject to supervision or oversight by Norges Bank

System		Instrument	Operator	Norges Bank's role	Other responsible authorities
Interbank systems	Norges Bank's settlement system	Cash	Norges Bank	Supervision (Norges Bank's Supervisory Council) and oversight	Supervision: Norwegian National Security Authority
	Norwegian interbank Clearing System (NICS)	Cash	Bits	Licensing and supervision	Supervision: Norwegian National Security Authority
	DNB's settlement system	Cash	DNB Bank	Licensing and supervision	Licensing and supervision of the bank as a whole: Financial Supervisory Authority and Ministry of Finance
	SpareBank 1 settlement system	Cash	SpareBank 1 SMN	Oversight	Licensing and supervision of the bank as a whole: Financial Supervisory Authority and Ministry of Finance
	CLS	Cash	CLS Bank International	Oversight in collaboration with other authorities	Licensing: Federal Reserve Board Supervision: Federal Reserve Bank of New York Oversight: Central banks whose currencies are traded at CLS (including Norges Bank)
Securities settlement systems	Euronext Securities Oslo's central securities depository (CSD) business	Securities and cash	Euronext Securities Oslo and Norges Bank	Oversight	Licensing and supervision of Euronext Securities Oslo: Financial Supervisory Authority
	LCH's central counterparty system	Financial instruments	LCH	Oversight in collaboration with other authorities	Supervision: Bank of England Oversight: EMIR College and Global College (including Norges Bank)
	Cboe Clear Europe's central counterparty system	Financial instruments	Cboe Clear Europe	Oversight in collaboration with other authorities	Supervision: De Nederlandsche Bank Oversight: EMIR College (including Norges Bank)

Definitions in the Payment Systems Act

Payment systems are interbank systems and systems for payment services.

Interbank systems are for the transfer of funds between banks with common rules for clearing and settlement.

Systems for payment services are for the transfer of funds between customer accounts in banks or other undertakings authorised to provide payment services.

Securities settlement systems are based on common rules for clearing, settlement or transfer of financial instruments.

Norges Bank assesses the FMIs that are subject to supervision and oversight in accordance with principles drawn up by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO).[2] The CPMI is a committee comprising representatives of central banks, and IOSCO is the international organisation of securities market regulators. The objective of the principles is to ensure a robust financial infrastructure that promotes financial stability.

A number of the FMIs that Norges Bank supervises or oversees are also followed up by other government bodies. The oversight of international FMIs that are important for the financial sector in Norway takes place through participation in international collaborative arrangements.

Finanstilsynet (Financial Supervisory Authority of Norway) supervises systems for payment services. These are retail systems that the public has access to, such as cash, card schemes and payment applications. The Central Bank Act from 2019 clarifies that Norges Bank's oversight covers the payment system as a whole, including retail systems that Finanstilsynet supervises. The preparatory works for the Central Bank Act state that in its oversight of the payment system, Norges Bank should be able to make appropriate use of Finanstilsynet's assessments of retail systems, especially with regard to their security.

The EU Central Securities Depository Regulation (CSDR) imposes a number of tasks on Norges Bank which supplement Norges Bank's responsibilities for overseeing Euronext Securities Oslo under the Central Bank Act. Finanstilsynet is the competent authority for Euronext Securities Oslo under the CSDR, while Norges Bank is a relevant authority.

A detailed description of the FMIs supervised or overseen by Norges Bank is provided in Norges Bank (2025c).

2 Principles for financial market infrastructures. See CPMI-IOSCO (2012).

Focus areas – Norges Bank's supervisory and oversight work

Prioritise strengthening resilience against severe cyberattacks.
In its supervision and oversight, Norges Bank will place greater emphasis on system owners' work to strengthen cyber resilience. This is particularly important in light of the rapid development of artificial intelligence and quantum technology. Norges Bank will review the cyber threat and risk assessments of FMIs. Furthermore, emphasis will be placed on institutions' contingency, continuity and incident management procedures, including plans for and execution of tests and exercises.

Prioritise contingency preparation for critical functions
Institutions must, to a greater extent, prepare for more serious incidents. In its supervision and oversight, Norges Bank will follow up and ensure the establishment of sufficiently independent contingency arrangements for critical functions.

Service provider dependency and supply chains
Norges Bank will follow up how institutions manage dependency on critical providers and supply chains. It is important that institutions' management and control of providers and outsourced activities are sound. Emphasis will be placed on the management of dependencies on shared critical service providers, as well as institutions' planning for management of risk of supply chain interruptions, including access to critical factors such as hardware and key expertise. Furthermore, the existence of realistic exit strategies in relation to critical providers is crucial.

References

Ahmed, R. and Aldasoro, I. (2026) Stablecoins and safe asset prices, BIS Working Papers No 1270

Bank of England (2025) Proposed regulatory regime for sterling-denominated systemic stablecoins, Consultation Paper

BIS (2025) The next-generation monetary and financial system, BIS Annual Economic report 2025

BIS (202b) Project Leap: quantum-proofing the financial system

Cipollone (2026) The digital euro in a fragmenting world: ensuring Europe's resilience and autonomy in payments, speech 1 April 2026

CPMI-IOSCO (2012) Principles for Financial Market Infrastructures (PFMI)

Finance Norway (2026) Veikart for en kvantesikker finansnæring | Finans Norge (Road map for a post-quantum financial industry (in Norwegian only))

Finanstilsynet (2026) Risiko- og sårbarhetsanalyse 2026 – Finanstilsynet.no

G7 CEG (2026) G7 Cyber Expert Group Releases Roadmap for Coordinating the Transition to Post-Quantum Cryptography in the Financial Sector | U.S. Department of the Treasury, news release 12 January 2026

IMF (2025) Global Financial Stability Report, October 2025, "Shifting Ground beneath the Calm"

McKinsey and Artemis Analytics (2026) Stablecoins in payments: What the raw transaction numbers miss

NIST CSRC PQC (202x) National Institute of Standards and Technology – Computer Security Resource Center – Post-Quantum Cryptography

Norges Bank (2023) Central bank digital currency – experimental testing in project Phase 4, Norges Bank Papers 2/2023

Norges Bank (2024) Survey on crypto-assets in Norway, Norges Bank Papers 2/2024

Norges Bank (2025a), Retail Payment Services 2024.

Norges Bank (2025b) Norges Bank does not currently recommend the introduction of a central bank digital currency News release 10 December 2025

Norges Bank (2025c), Norway's financial system

Norges Bank (2026a) Central bank digital currency – final report for project Phase 5, Norges Bank Papers 1/2026

Norges Bank (2026b) Assessment of the potential consequences for Norway of the introduction of a digital euro, Norges Bank Papers 2/2026

Norges Bank (2026c) Central bank digital currency – experimental testing in project Phase 5, Norges Bank Papers 3/2026

Norges Bank (2026d) Survey on crypto assets in Norway, Norges Bank Papers 6/2026

Norges Bank (2026e) Husholdningers bruk av og holdninger til kontanter [Households' use of and attitudes towards cash]. Norges Bank Papers 7/2026 (in Norwegian only).

NSM (2023) Kvantemigrasjon – veileder – Nasjonal sikkerhetsmyndighet (Quantum migration – guide – National Security Authority (in Norwegian only)).

NSM (2026) Position paper on quantum key distribution (in Norwegian only)

Norges Bank
Financial Infrastructure Report 2026
Oslo 2025

Address: Bankplassen 2
Postal address: P.O. Box 1179 Sentrum, N-0107 Oslo, Norway
Phone: 22 31 60 00
E-mail: central.bank@norges-bank.no
www.norges-bank.no

Editor: Ida Wolden Bache

Design: TRY
Layout: Aksell AS
ISSN 1894-8634