Norges Bank

3 | 2023

Norges Bank Papers

Central bank digital currency – experimental testing in project Phase 4

REPORT FROM A WORKING GROUP

Contents

1. Introduction and summary

This is a sub report from phase 4 of Norges Bank's central bank digital currency (CBDC) project. The project began in 2016. Reports from former phases are available on Norges Bank's websites.

Norges Bank has not decided on whether to introduce a CBDC, nor on the type of technology and design.

In Phase 4 of Norges Bank's CBDC project, the work relating to the validation of technical solutions was supplemented by experimental testing. This work was carried out by a Validation Group (VG).[1] This report discusses the experimental technology testing.

The purpose of this work was to validate various technologies' ability to deliver characteristics required for a CBDC to fulfil its objective.[2] The work served also as a basis for dialogue with the industry, other authorities and other central banks. Furthermore, the validation work has contributed in building expertise necessary to assess how the CBDC-related work should be pursued.

Besides using Norges Bank's internal resources, an external project coordinator has assisted in the validation work. Four IT companies have been engaged to develop applications for testing of the characteristics. In addition, Norges Bank engaged a student for programming tasks. Norges Bank has also been in contact with students who have completed student projects and written CBDC-related master's theses.

In the context of this work, Norges Bank has engaged in dialogue with several private market participants (including Norwegian and international technology companies and financial institutions such as banks established in Norway), the authorities, other central banks and international organisations, such as the BIS Innovation Hub (BISIH). Moreover, Norges Bank has reported on its CBDC project at numerous conferences and seminars and has organised two conferences and three hackathons in cooperation with other entities.

The experimental testing was conducted by constructing some test cases that validate aspects of one or more characteristics. The testing was mainly conducted in a prototype/sandbox based on open source and blockchain technology (private Ethereum network) developed by one of the IT companies. The experimental testing is deemed to be successful according to the objectives of the testing, including delivering on the list of characteristics in Table 1. In addition to the actual validation, the testing has been a springboard for collaboration with various stakeholders.

The choice of technology, including the use of known technology based on open source, has constituted an important factor in achieving the objectives. If a more

[1] The group has comprised Peder Østbye (head), Espen Gjøs, Helge Syrstad, Terje Åmås, Suela Kristiansen and Kjetil Watne. Suela and Kjetil joined sometime after the work had been initiated. In addition, Lasse Meholm from the company Finansit has participated as external project coordinator. Knut Sandal and Anette Monshaugen have participated in activities by VG as associate members. The IT companies mentioned in the text are Nahmii, Symfoni, NBX and Alpha Venturi.

[2] The characteristics are defined in Norges Bank Papers 1/2021.

unknown and/or proprietary technology had been selected, one would unlikely have achieved the same results.

Many tests were conducted. At the same time, continued experimental testing involving the establishment of new test cases and further development of existing test cases in the next phase may provide additional insight necessary for any introduction of a CBDC. Among other elements, data protection and privacy solutions and solutions for regulatory compliance may need further exploration. Test cases can also be designed for performance testing (e.g., number of transactions per second and time to final settlement) and security testing. There is also a need to test incentive structures and new business models for third parties (including banks), retailers and consumers.

The testing has revealed that different types of technologies and ways of maintaining registers/ledgers offer different features that to varying degrees can deliver the required characteristics of a CBDC. In order to exploit advantages and disadvantages inherent in different register/ledger solutions, a potential solution may be to use several registers/ledgers linked together through bridges. The relative advantages of different types of registers can be exploited by means of such bridges. However, bridges raise some unique challenges highlighted in the experimental testing.

Norges Bank's strategy up to 2025 states that the central bank will prepare the ground for the issue, if appropriate, of a CBDC. This will entail both assessing the need for and consequences of introducing CBDC and obtaining information concerning solutions that can be introduced and recommended for potential implementation.

The VG's assessment based on the described test work and information obtained from suppliers of CBDC solutions to other countries, is that as of today, readymade solutions (otherwise called "off-the-shelf" or white label solutions) that can successfully meet the requirements/deliver necessary characteristics of a Norwegian CBDC are not yet fully satisfactory.

Developing a full-scale CBDC solution is a major task, and the working group is of the opinion that it would be unlikely for Norges Bank to develop a full-scale solution on its own given the resources that it requires.

CBDC technologies are rapidly evolving, and more suitable solutions will probably be developed in the course of the strategy period, both in the market and as a result of development work at other central banks. Developments at other central banks may also represent relevant technology for a potential Norwegian CBDC.

In addition to this report, a final report on the project's Phase 4 work will be published as a *Norges Bank Papers* 2/2023[3]. A *Norges Bank Staff Memo* on the

[3] Norges Bank Papers (2/2023). «Central bank digital currency – final report from Project Phase 4. Report from a working group».

consequences for liquidity management and monetary policy will be published as well.[4] *Staff Memo*[5] on legal assessments of CBDC has previously been published.

2. Method applied in the validation work

The validation work has consisted of experimental testing and analyses. The purpose has been to investigate whether technical solutions can deliver the characteristics in Table 1 identified in *Norges Bank Papers* 1/2021.

Table 1: Necessary characteristics of a CBDC, identified in *Norges Bank Papers 1/2021*

E1	Claim on Norges Bank
E2	Parity value with cash and bank deposits
E3	Customer orientation
E4	Adequate frictions between the CBDC and bank deposits
E5	Controlled by Norges Bank
E6	Capable of functioning as legal tender
E7	Compliant with obligations under EEA law
E8	Payments are immediate and final
E9	Compliant with sound IT architecture principles
E10	Satisfy requirements relating to technical independence and offline payment functionality
E11	Customer communications and due diligence undertaken by third parties
E12	Flexibility to accommodate different data protection solutions
E13	Platform for third-party providers/innovation
E14	Safeguard monetary policy efficacy
E15	Information relevant to Norges Bank's macroeconomic monitoring
E16	DLT compatible
E17	Attractive niche solution

The testing has been conducted using test cases since it is difficult to test the characteristics directly. The characteristics have therefore been indirectly tested by means of test cases that cast light on whether the characteristics are delivered (see Figure 1).[6]

[4] Bernhardsen, T. og Kloster, A. (2023). Central bank digital currency – implications for liquidity management and monetary policy. Norges Bank Staff Memo, https://www.norges-bank.no/en/news-events/news-publications/Papers/Staff-Memo/2023/sm-19-2023-cbdc/

[5] Syrstad, H. (2023). «Introduction of central bank digital currency – necessary legislative amendments», Norges Bank Staff Memo 4/2023, https://www.norges-bank.no/en/news-events/news-publications/Papers/Staff-Memo/2023/sm-4-2023-cbdc/

[6] The test cases have therefore been an analytical mediator between the technology and the characteristics.

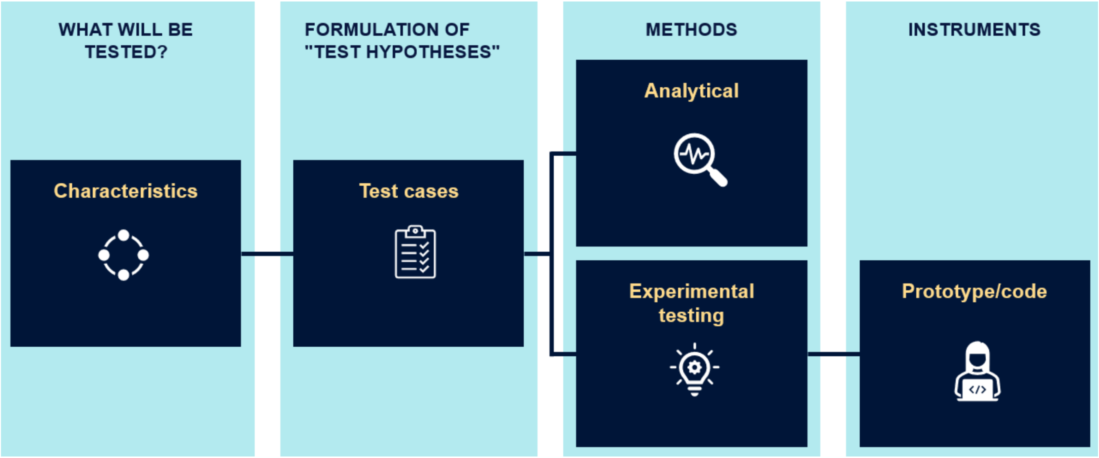


Figure 1 Conducting a test

Source: Norges Bank

Analysis work and experimental testing have complemented each other. In areas where we have not tested sufficiently, such as, for example, in the area of offline solutions, the project has benefited from external work. This includes both analytical work and tests conducted by others. Our own experimental testing has also served as an additional source for analyses conducted by others, thereby enabling the diversity of sources and testing methods as well as the quality assurance of results.

The process has also been iterative. This has implied prioritising tests or the designing of new test cases, as illustrated in Figure 2 below. Conducting some test cases has, among other things, brought new uncertainties into focus, which have been reduced by new test cases.

As Figure 2 indicates, some tests have been conducted by designing test cases based on different functional areas for CBDC. This reduces uncertainty about whether the characteristics can be assured. The issuance and destruction of a CBDC as described in Section 3.3(A) below is an example of a test case. The issuance and destruction of a CBDC was necessary in order to test the characteristics. We prepared a requirement specification for the element to be developed and then received a prototype developed by contracted IT consultants. Subsequently, we tested the prototype. Finally, we assessed the result and identified remaining uncertainty. By starting with a need, we were also able to assess whether the characteristics in Table 1 were assured.

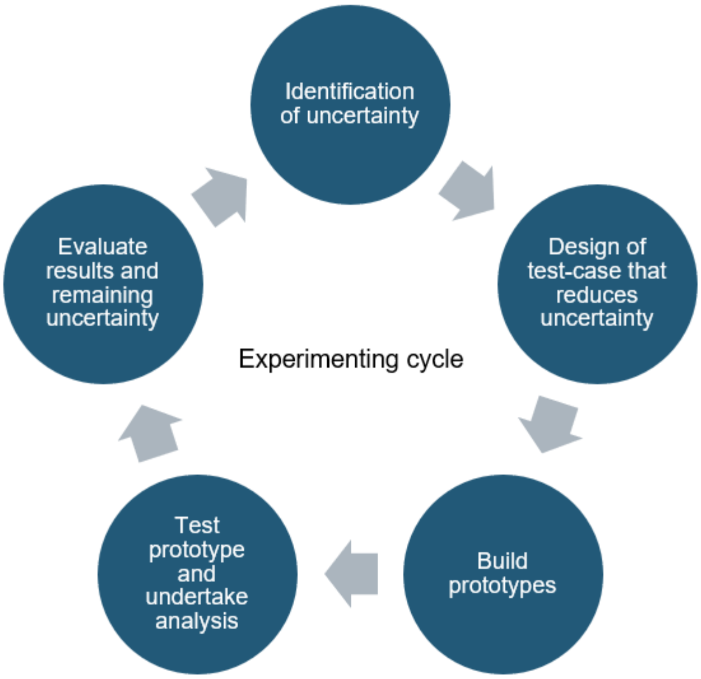

Identification of uncertainty
Design of test-case that reduces uncertainty
Build prototypes
Test prototype and undertake analysis
Evaluate results and remaining uncertainty
Experimenting cycle

Figure 2 Experimentation cycle

Source: Norges Bank

The test cases were mainly conducted with the support of a prototype based on a private Ethereum network and open source called Hyperledger Besu. This technology is described below in further detail. The use of open source code facilitated the sharing of work and the involvement of Norwegian fintech and innovation environments. In September 2022, the source code for the prototype was made public on GitHub, which formed the basis for a technical sandbox that participants in the testing – both internal and external – could make use of.

We also conducted more limited tests of other technologies, including OpenCBDC, which is an open source infrastructure developed by the Massachusetts Institute of Technology (MIT) in collaboration with the Boston Fed.

As part of the testing, Norges Bank financed development projects and participated in collaborations with stakeholders that had the desire and capacity to participate in the testing. These stakeholders included banks and other payment providers, including fintech companies, government agencies, and academia. A multitude of market participants and stakeholders have thus participated in or contributed to the testing in various ways.

VG adopted an open approach and held meetings with a number of market participants during which work-related information was provided. Together with these market participants, we arranged, in the course of autumn/winter of 2022-23, among other things, two conferences combined with a hackathon/ideathon in addition to a brainstorming session.

3. Conducting experimental testing

3.1 Choice of technology for the experimental testing

Norges Bank Papers 1/2021 recommended testing several technologies, which also follows from the validation work mandate. There was a particular need to test the technology in token-based solutions. This technology shares some similarities with cryptocurrencies/blockchain-related technology, and that builds further on innovations in cryptography and distributed ledger systems.

Its potential to replicate important characteristics of cash, including representing an independent infrastructure for central bank money available to the public, and at the same time making it possible to use central bank money for online/remote payments, is an important motivation for testing token technology. In addition, digital token-based money can offer innovative functionality such as programmability. However, there is uncertainty surrounding such technology, and more knowledge is required before one may conclude on this technology's suitability for a potential CBDC solution in Norway. Hence, in the context of the experimental testing this technology has received particular attention.

As mentioned, the experimental testing mainly used open source technology. This technology was used for several reasons. Much of the technology pertaining to cryptocurrencies and token-based solutions is based on open source and there are many development environments, also in Norway. Open source also provides the freedom to conduct testing without relying on access to individual market participants' proprietary technologies. This simplifies and increases flexibility in the cooperation with suppliers and other stakeholders. Furthermore, a number of available mathematical models and simulation tools can supplement the testing. While open source will not necessarily be selected for a potential final CBDC solution, considerable knowledge transferable to other technologies can be gained through open source.

Below is an overview of the technologies used in the experimental testing.

Ethereum technology
Ethereum is known as an open and public blockchain with the embedded cryptocurrency Ether. However, private variants of Ethereum without any associated cryptocurrency also exist, such as Hyperledger Besu. In a blockchain network such as this, so-called nodes are found installed on computers. Nodes ensure transaction validation (presence of money in the payer's "account" and signing of the transaction) and smart contract processing. The nodes in the network can be operated in a centralised or decentralised manner. Although the network/register/ledger does not use an open and public blockchain, other forms of Ethereum technology may be used. A private variant of Ethereum such as this was used for the developed prototype/sandbox and as test cases' starting point. This implies that the payment system is implemented in a test network of nodes using the Hyperledger Besu software.[7]

[7] https://www.hyperledger.org/use/besu

This technology involves money being represented by a so-called ERC-20-token.[8] This means that money is represented as balances at register/ledger addresses similarly to bank accounts. These register addresses could potentially be linked to identifiable individuals through a separate database (alias base, see 3.3.E).

The technology facilitates the programming functionality (i.e. implementing smart contracts) offered on Ethereum (through the "Ethereum Virtual Machine"-EVM).[9] Programming functionality means that computer programs can be run in/on the register.[10] Among other things, programming functionality can facilitate conditions for issuance and destruction, anonymous payments (using cryptography), and conditional payments (payments that depend on the occurrence of one or several predefined conditions).

A substantial amount of complementary software has been developed in the "market" (also based on open source) including digital wallets, privacy solutions, analysis tools and systems for regulatory compliance. Complementary software such as this has been employed in the testing.

Many so-called stablecoins and infrastructures within blockchain technology have chosen to utilise, among other things, ERC-20-tokens and Ethereum's programming language, so that the technology is relatively well-tested. Various infrastructures that can be combined with Ethereum technology are therefore being rapidly developed. Hyperledger Besu and the ERC-20-token are also used by other central banks and the BISIH for CBDC testing.

OpenCBDC/Project Hamilton

OpenCBDC/Project Hamilton[11] is a collaboration between the Federal Reserve Bank of Boston[12] and the MIT Digital Currency Initiative.[13] In an initial phase, they tested the capacity of certain alternative infrastructures. In this testing, money has a slightly different representation than in the Ethereum technology used in our prototype. Values are represented by tokens at the owner's disposal using cryptographic codes following a valid transaction chain (so-called Unspent Transaction Output – UTXO)[14] from original issuance. The money therefore does not accumulate in balances as is the case in the Ethereum technology described above. Different Bitcoin variants and several other cryptocurrencies use this type of value representation.

The software that the Hamilton project uses in its testing is based on open source code that was made available for external testing. Several other central banks have taken the opportunity to conduct tests using this source code. Our CBDC project has only involved conducting a few very limited tests of the OpenCBDC technology. One

[8] https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. ERC stands for "Ethereum Request for Comments".

[9] https://ethereum.org/en/developers/docs/evm/

[10] The fact that an arbitrary program can be executed means that EVM is so-called "Turing-complete", which means that any potential program can be run.

[11] https://dci.mit.edu/project-hamilton-building-a-hypothetical-cbdc

[12] https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx

[13] https://dci.mit.edu/

[14] https://www.ledger.com/academy/glossary/unspent-transaction-output-utxo[15] https://www.bis.org/about/bisih/about.htm

of the features of the OpenCBDC technology is that it can process 1.8 million transactions per second, which may be crucial for large countries like the US.

Information gathering on technology used by commercial off-the-shelf suppliers. Some private market participants have developed CBDC solutions that have been put into production or are included in pilot tests. The BISIH[15] has participated in several of these pilot tests. Some of the solutions are based on Ethereum technology, others are based on variants of UTXO, while some have developed their own independent technologies. The solutions have various elements of proprietary technology.

As part of the experimental testing in this phase, the project involved some aggregated-level tests of two of such commercial off-the-shelf-suppliers' solutions. This provided insight into the technologies, how the solutions work end-to-end and provided a basis for benchmarking the technologies against the prototype developed by Norges Bank itself. Specifically, we conducted workshops with two different international market participants.

The interaction between money representations and registers (bridges and swaps). An overall experience from the testing work is that there is unlikely to be one type of register/ledger or technology that covers all CBDC-related needs. Different types of registers and technologies cover different functions and needs, such as programmability, mass payments, machine-to-machine (M2M) payments and offline payments.

Different registers may also have different access rights. For example, it is conceivable that only Norges Bank, other central banks and banks would have access to the register where a CBDC is issued and destroyed – so that in practice this core register functions as a so-called wholesale CBDC (wCBDC – CBDC for settlement, only available to actors with an account at the central bank) that is converted into a retail CBDC (rCBDC – CBDC that is available to the public) in other registers/ledgers.

In principle, it is also imaginable that a CBDC can be transferred to private registers (using a bridge), including decentralised registers, even if this raises some issues. Thus, testing the so-called bridges between different registers was important in the testing process. In simple terms, a bridge implies that you can transfer CBDC tokens from one register to another, so that different types of registers can function together. A multitude of registers/ledgers linked together through bridges represents one potential type of holistic architecture that may be generalised from the test cases.

As part of the process of testing bridges, we tested how a CBDC can be represented by and exchanged between different tokens within the Ethereum technology on which the prototype is built (a so-called swap). Testcase 3.3.C is an example of this type of bridge.

[15] https://www.bis.org/about/bisih/about.htm

Another type of bridge that was tested is a bridge between the prototype and a register based on IOTA technology (test case 3.3.H). IOTA is a payment system based on decentralised technology, specially adapted for the Internet of Things (IoT) and automated processes that execute transactions in large volumes with small amounts and make financial settlement/payment without manual intervention. Token-based money that is programmable works well in such a mechanism.

3.2 The development of the prototype

Following a tender competition in spring 2022, one of the mentioned IT companies was tasked with developing a prototype infrastructure based on a private Ethereum network as described above, in order to conduct test cases. In this document, the prototype is also referred to as a sandbox. The source code was published on public Github in September 2022.

The company was also tasked with running the network on behalf of Norges Bank. This implied that the company designed six nodes, each containing a full version of the register/database/ledger with all the transactions. The multi-node setup contributes to redundancy and reduces the risk of downtime if single nodes fail.

The prototype is configured so that transactions initiated by the users are collected in blocks (blockchain) that are added to the register every five seconds. The transactions are added to the register and consolidated between the nodes using a consensus mechanism based on Proof-of-Authority (PoA). This signifies that the nodes, which are under Norges Bank's control but operated by the IT company, validate and approve all transactions added to the register. This represents a significant difference compared to open blockchains used in Bitcoin, for example, where a consensus mechanism is required that enables everyone to participate in the validation of transactions in a decentralised manner without the need for a central player to run the register (so-called Proof-of-Work, PoW). However, the technology in the prototype enables more decentralised validation methods (consensus mechanisms) if desired. PoA requires very little energy/cost compared to PoW. We also chose to let payments be free, without so-called gas fees (transaction cost) in the context of Ethereum.

Figure 3 shows the overall architecture of the prototype.

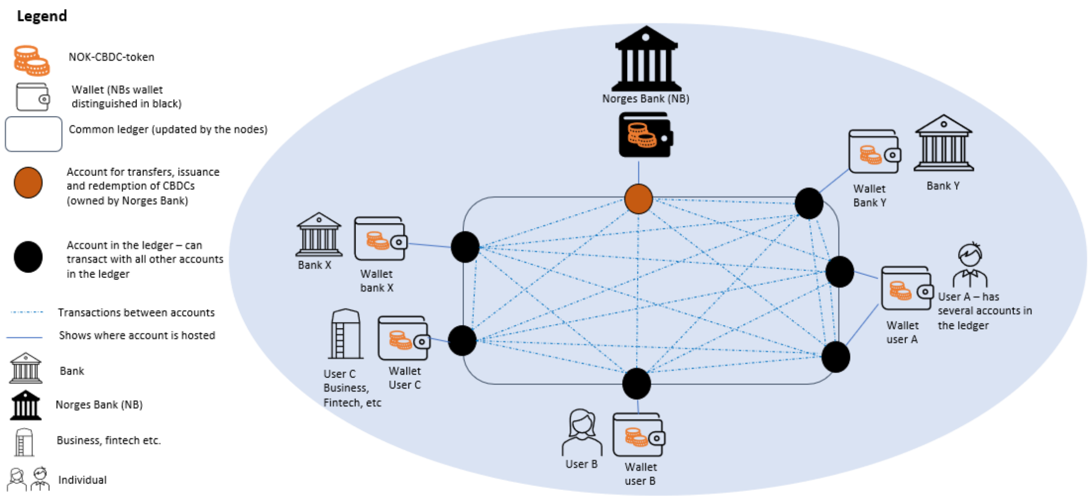

Legend
NOK-CBDC-token
Wallet (NBs wallet distinguished in black)
Common ledger (updated by the nodes)
Account for transfers, issuance and redemption of CBDCs (owned by Norges Bank)
Account in the ledger – can transact with all other accounts in the ledger
Transactions between accounts
Shows where account is hosted
Bank
Norges Bank (NB)
Business, fintech etc.
Individual
Norges Bank (NB)
Wallet Bank Y
Bank Y
Bank X
Wallet bank X
User A – has several accounts in the ledger
Wallet user A
User C Business, Fintech, etc
Wallet User C
User B
Wallet user B

Figure 3 Visualisation of the prototype

Source: Norges Bank

Access to the test environment is possible through a password, and external market participants who wished to participate in the testing were assigned participation usernames and passwords. To interact and use the register, the user must have a digital wallet. We chose to use a soft-wallet with keystore file containing the users' cryptographic codes in a password-protected file.[16] The wallet stores the users' codes and is therefore a digital wallet without a manager (known as self-hosted/self-custodial wallet).

In principle, all users are equal. This means that all users have access to the register and can send transactions from one to the other, and view transactions in the register with a so-called Block Explorer.[17] Although initially all users are equal, this can be altered by taking advantage of the programming functionality inherent in EVM.

In the prototype, only Norges Bank can issue and destroy (mint and burn) CBDC. The underlying idea is that Norges Bank transfers CBDC to banks and potentially other private market participants, which in turn distribute CBDC to their customers. This is called two-layer architecture. Different access levels have been explored further in some of the test cases.

The prototype was not developed with a view to later becoming a production solution for a CBDC. This would require extensive further development and testing. For example, performance tests or security tests of the prototype were not conducted, and these would be important for a production solution. Numerous experimental and analytical works carried out by others exist that shed light on these aspects of the technology more generally. Such testing could potentially be part of subsequent work.

[16] An alternative is to use a so-called seed phrase, i.e., a randomly generated sequence of words that deterministically generate private keys. The user must then memorise this series of words to recreate the cryptographic keys.
[17] BlockScout was used as a block explorer in testing.

3.3 Test cases related to the prototype

Table 2 provides an overview of the test cases that were conducted associated with the prototype and the characteristics tested in the test cases. Some of the test cases were relevant regarding several characteristics, while others covered "only" one of the characteristics. Nevertheless, this does not imply that all aspects of its characteristics were tested.

Test streams	Test cases	Range of properties tested
i) Development of prototype infrastructure based on private Ethereum network (open source)	A. Issuance and destruction of CBDC	E1, E5, E8, E9, E11, E15, E16
	B. Transfer to and between digital wallets	E1, E5, E8, E9, E11, E15, E16
ii) Further development and functionality of prototype infrastructure	C. Transfer between token standards	E3, E13, E16, E17
	D. Mass payments	E3, E6, E11, E16, E17
	E. Alias base	E3, E7, E11, E12, E16
	F. Digital identity/ eIDAS2	E3, E7, E12, E11, E12, E16
	G. Calculation of interest	E4, E14
	H. Bridges between the CBDC in the prototype and other registers	E7, E13, E16, E17
	I. Payment amount and holding limits	E13, E17
	J. Anti-money laundering	E7, E11
	K. Anonymous payments	E3, E7, E12, E17

Table 2 Overview of test streams and test cases

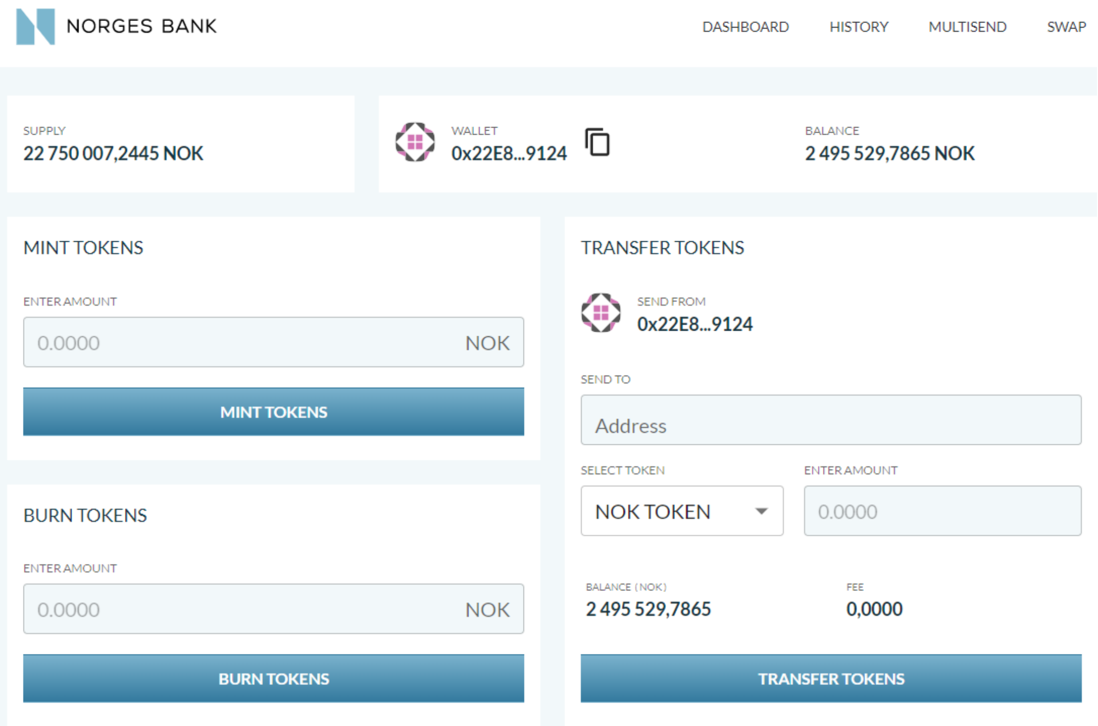
i. Development of prototype infrastructure based on private Ethereum network (with open source)

Establishment of sandbox, nodes, digital wallet with user-interface for Norges Bank and banks.

A. Issuance and destruction of CBDC

This test case is linked to several desired characteristics of a CBDC, including the idea that only Norges Bank can issue and destroy CBDC. The digital wallet that was developed granted Norges Bank sole rights to issue and destroy CBDC. A simple digital wallet and dashboard were also developed for central bank monitoring of blockchain and circulation of CBDC. Figure 4 shows a screenshot of the user interface. As shown in the picture, it is possible for Norges Bank to issue ("mint") and destroy ("burn") CBDC tokens.

The test confirmed that only Norges Bank could issue and destroy CBDC. The screenshot below shows "Balance" in the upper right, which is how much CBDC the central bank has in its holdings, and "Supply" in the upper left shows the value of CBDC in circulation.



SUPPLY
22 750 007,2445 NOK

WALLET
0x22E8...9124

BALANCE
2 495 529,7865 NOK

MINT TOKENS

ENTER AMOUNT
0.0000 NOK

BURN TOKENS

ENTER AMOUNT
0.0000 NOK

TRANSFER TOKENS

SEND FROM
0x22E8...9124

SEND TO
Address

SELECT TOKEN
NOK TOKEN

ENTER AMOUNT
0.0000

BALANCE (NOK)
2 495 529,7865

FEE
0,0000

Figure 4 Screenshot from Norges Bank's digital wallet

B. Transferring to and between digital wallets

In the prototype, it is possible to transfer NOK tokens from one register address (account) to another. The balance is continuously updated. It was tested with multiple addresses and transactions and conducted in real time (immediate and final payments). This can be a peer-to-peer payment between two people possessing CBDC wallets. It may also be two businesses that pay to each other or a customer who pays physically in stores or online. This is indicated on the right side in the screenshot in Figure 4.

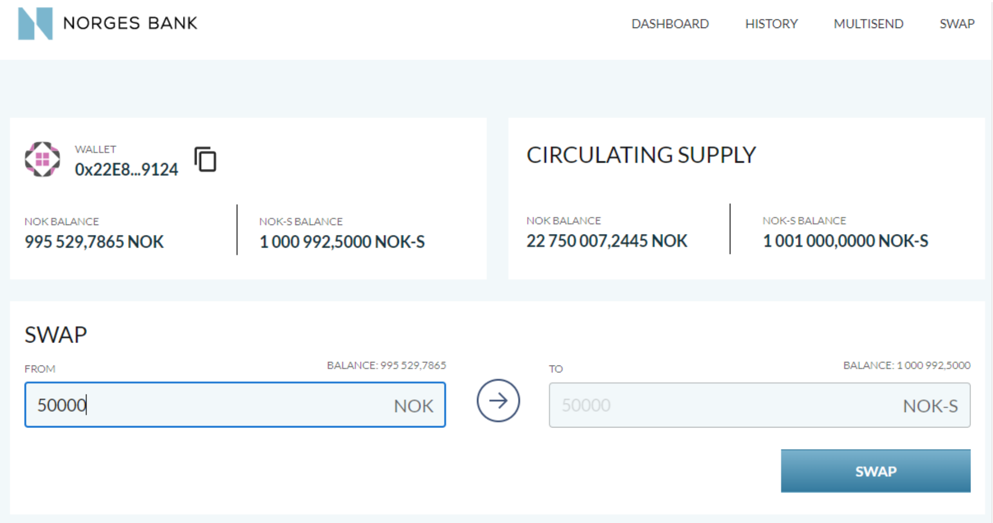
The test confirmed that transactions between digital wallets could be carried out.

ii. Further development and functionality of prototype infrastructure

C. Transfer between token standards – bridges

The purpose of this test case was to investigate whether tokens can be transferred between registers with different token standards within the prototype. This is an example of testing whether tokens can be transferred from one technology to another without alteration of characteristics. Diverse token standards may present various advantages and disadvantages. For example, built-in programming functionality and information that can accompany the token may be different. For example, one type of token can be particularly useful in retail loyalty programs.

In the test case, CBDC was converted in real time from one type of token to another (as in the example referred to here – from ERC-20-token to ERC-1400-token). By bridging/swapping, the amount of tokens available in the different networks/eco-systems is adjusted in real time in different forms: conversion from ERC-20-token to ERC-1400-token occurs by locking the token in the ERC-20 (locked) network and simultaneously issuing (minting) a token in the ERC-1400 network. NOK is returned by destroying (burning) the token in the ERC-1400 network and unlocking the same value in the ERC-20 network.



WALLET 0x22E8...9124

NOK BALANCE 995 529,7865 NOK

NOK-S BALANCE 1 000 992,5000 NOK-S

CIRCULATING SUPPLY

NOK BALANCE 22 750 007,2445 NOK

NOK-S BALANCE 1 001 000,0000 NOK-S

SWAP

FROM — BALANCE: 995 529,7865 — 50000 NOK

TO — BALANCE: 1 000 992,5000 — 50000 NOK-S

Figure 5 NOK token exchanged with S-NOK-token

The test confirmed that it was possible to transfer CBDC between registers based on different standards.

D. Mass payments

The purpose of this test case was to investigate whether the prototype could be used for mass payments. Such a feature can help make a CBDC an efficient and customer-friendly payment solution for payments to many recipients in a single process. As demonstrated by the example below, it can also make a CBDC an attractive niche solution for special payment situations.

It should be possible to use the solution for mass payments to several million payees, but for practical reasons we chose to limit it to around 200. Further testing with multiple payees will depend on further development of the sandbox with valid addresses of multiple payees' digital wallets.

Such a function may be relevant, hypothetically, in connection with the payment of support for electricity bills. For example, in the form of a support payment of NOK 500 towards electricity bills to all with an income of less than NOK 750 000 and more than two children (this will require integration with, for example, tax data in order to automatically identify who is eligible for such support). In such cases, CBDC payments may be considered.[18] Salary payments from large companies is another example.

Although this test was conducted with mass payments to a limited number of payees, the functionality can also be used for payments to a much greater number of payees.

E. Aliasbase

Validating the possibility of linking payments to the owner of a digital wallet was the purpose of this test case. A solution was developed with a database (MYSQL) located on a server outside the blockchain (off-chain) where information about the owner of the wallet with name, national identity number and mobile phone number was stored. This allows a payer to bring up the name of the payee on the payment screen to avoid paying to the wrong person. Such a database can and should potentially be stored at each bank that is the customer's main bank (as is the case today), and is responsible for conducting KYC/AML ("Know Your Customer" /"Anti Money Laundering") in a secure manner, pursuant to obligations under EEA law. This also confirms that it is possible to distinguish private information from payment transactions.

The test confirmed that linking to an aliasbase is possible.

F. Digital Identity/ eIDAS2

The EU is working on solutions for digital identity and wallet related to the eIDAS2-regulation (the use of eIDAS2-regulation[19] is also known as verified credentials, (VC)/ "verified identity"). A solution was developed in collaboration with the

[18] Several regulatory issues are related to this test case. If foreign workers do not have the ability to identify themselves, access to a CBDC can be problematic in relation to the AML rules. However, one might consider that in some cases, standardised European access (for example, as expected with eIDAS2) may reduce barriers. In addition, even if an authentication solution is implemented, foreign actors may lack access to CBDC.

[19] eIDAS stands for «**E**lectronic **ID**entification, **A**uthentication and Trust **S**ervices Regulation». More information on EIDAS can be found here: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation and here: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

Norwegian Digitalisation Agency (Digdir) that uses the same mechanism as eIDAS2 by developing a so-called oracle in connection with the ID portal. This makes it possible to verify that a person truly is who they claim they are. It can simplify and improve the work with KYC and AML for banks and third parties. Our solution in the test took advantage of the fact that CBDC is programmable where the money is programmed (smart contract) to not be owned by someone without a verified identity. As far as we know, Norges Bank is the first central bank in the world to test such a possibility.

Digital identity is a prerequisite for making digital payments securely and for reducing the risk of CBDCs being used for money laundering and the financing of terror. The payer and payee must be known, and the origin of the funds must be documented. Cross-border payment challenges are increasing. Various countries offer different solutions, and up to now standardisation remains limited. This topic is widely discussed internationally.

The test confirmed that verification of identity via VC was possible.

G. Interest calculation

The purpose of this test case was to shed light on the possibility of calculating interest on CBDC holdings. It has not been decided whether or not Norges Bank wishes for any CBDC to earn interest. The project had nevertheless been commissioned to test whether interest on CBDC was technically feasible. Both positive and negative interest on CBDC were developed and tested. The project therefore was able to program and test interest on CBDC in the sandbox. Testing showed that it was possible to perform interest calculations over a simulated period of two years, entailing various interest rate changes, and with both positive and negative interest rates.

In the conducting of the test, we chose to exploit opportunities provided by new technology for performing interest calculations. Instead of calculating interest periodically, for example once a year, we chose continuous interest. The interest calculation was developed based on the architecture of the DeFi protocol Aave[20]. Interest calculation was added into the smart contract in the ERC-20-token, thus we also tested the CBDC's programmability. This means that the money calculates the interest itself, not the central bank or banks. Interest is essentially calculated at the completion of each transaction. The balance in the digital wallet is multiplied by the interest rate per second, which in turn is multiplied by the number of seconds gone by since the last transaction. The resulting interest in Norwegian kroner can be spent immediately by the owner of the digital wallet. The interest rate will be set by the central bank.

A solution was also developed that can update the pre-completed tax settlement at the end of the year with interest for the year just ended, as banks do today, if necessary.

[20] https://aave.com/

Interest can be used as a mechanism to influence incentives to hold CBDC and thereby regulate the volume of CBDC in the population. For example, negative interest on CBDCs will reduce the desire to keep money in the CBDC wallet.

In another test case, we tested maximum limits on CBDC per person in different variants.

This test case showed that it was possible to calculate interest in real time via the Aave protocol.

This interest calculation is an example of programming[21]. Programming can be at the core or at the top of the token as in the case of payments' services (for example, conditional payments). Programming can in some situations also have negative consequences, while it can give possibilities in many contexts of use. Further testing of programmable CBDC should therefore be accompanied by an analysis of consequences.

H. Bridges between CBDC in the prototype and other registers

The purpose of this test case was to test the transferability of ERC-20 tokens using a bridge to another register[22] in which the tokens are represented as UTXO. IOTA is one such technology. IOTA technology is specially developed for IoT and M2M payments that involve very small amounts (micropayments) but in large volumes. Many see this as a necessity for business models of the future, where, among other things, payment takes place simultaneously with consumption. Examples are road use payments per distance travelled in cities while driving, instead of toll payments billed once a month, which are largely used today, or two machines communicating about producing a product and paying each other in real-time. A bridge between ERC-20 and UTXO facilitates further testing of offline solutions.

One challenge in conducting this test was that technology in IOTA (EVM compatibility through a so-called "layer 2", L2) to implement such bridges was not fully developed. Using assumptions and simulation, it was nevertheless possible to conduct the test case.

I. Payment amount and holding limits

Two different limits were tested. The first limit is a maximum holding limit, i.e., on how much CBDC a user can have in his or her digital wallet. In a production solution, the excess will be sent to the customer's bank account. In order to replicate a bank account, a separate digital wallet address was designed to which the excess was sent. A limit on amounts paid per week was also tested. In a real system, it may also be relevant to set a limit on amounts and transaction limits per day, week, month, etc. However, a limit per week was sufficient to test the mechanism.

[21] Look at https://www.bis.org/publ/bisbull72.htm for a discussion of several aspects related to the programmability of tokens.

[22] This contrasts with the swap discussed above where the test case was to move tokens between different token standards in the same register.

The tests confirmed the possibility of setting payment amount limits and holding limits for wallets.

J. Anti-money laundering etc.

Banks and other payment service providers (PSPs) in Norway and abroad are subject to special statutory rules for measures pertaining to AML, detection of tax evasion and anti-terrorist financing (known as “Counter Financing of Terrorism”, CFT). Society needs to protect itself against payments from illegal activities. At the same time, society needs good privacy protection and all types of organisations that process information that can be linked to individuals in the EU/EEA are subject to regulations such as the General Data Protection Regulation (GDPR). Different considerations, needs and requirements must therefore not be seen as isolated, by weighed against each other.

In the work on testing CBDC at Norges Bank, some tests related to these challenges were conducted, primarily to gain experience regarding opportunities the technology has to offer. First, it was tested whether transactions can be monitored in a structured manner to automatically detect possible suspicious transactions. It was also tested whether amounts below a certain limit are not subject to monitoring, provided that too many small transactions are not carried out within a certain time. As the prototype uses a pure blockchain technology, it is possible to monitor both payer and payee during the same process. The project also included testing the possibility of hindering suspicious payments in real time before they reach the payee. Finally, it was tested whether it is technically possible to seize funds and transfer assets to a digital wallet, which could for example be owned or controlled by the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim).

The tests confirmed the possibility for the facilitation of several AML/CFT-related processes.

As described below (test case K), testing anonymous payments was also part of the project. Anonymous payments can technically affect how efficiently the AML/CFT mechanism functions.

K. Anonymous payments

Privacy as mentioned, is an important CBDC-consideration. Individuals’ right to privacy must be balanced against requirements related to AML/CFT regulations. Whether some payments should be entirely anonymous is a broadly discussed topic in international forums on CBDC. Some central banks have suggested that payments below a certain threshold could be entirely anonymous. Regardless of the acceptance of anonymity associated with payments in Norway, a need to test the technology’s potentials exists.

The project involved testing the possibility of anonymity for all payments, alternatively anonymity for payments below a certain limit. One of the technologies investigated was based on zero-knowledge proof (ZKP). Another was the so-called tornado cash mechanism. The technology that was tested the most was based on the Basic stealth addresses[23] mechanism. Technologies for anonymous payments are evolving and a perfect solution does not currently exist. For example, the widely used ZKP can raise challenges for CBDC programmability. The conclusion of the test is that the technology used can enable anonymous payments, to the extent that one wants to cater for this.

3.4 Cross-border CBDC payments

Project *Icebreaker*[24] was initiated in 2022 in collaboration between Norges Bank, Sveriges Riksbank (the Swedish central bank), the Bank of Israel and the BISIH Nordic Centre. In the context of the project a technical solution for cross-border CBDC payments was developed. The three central banks' Proofs of Concept (POCs)/prototypes were linked together through a common hub for sending communications/messages related to cross-border CBDC payments, between wallet providers and several foreign exchange market participants.

The project contributes to the CBDC-related work in several ways:

1. It demonstrates the ability of CBDC to streamline and simplify multi-currency cross-border payments;
2. It tests for the interoperability of the current prototype with several CBDC prototypes from other countries;
3. It shows that it is possible to make cross-border payments even if different countries use different CBDC technology[25];
4. It presents a test case for FXPs[26] in which the means of settlement can be in the CBDC in the jurisdictions where they operate;
5. This shows that it is technically feasible to foster competition between several institutions to deliver the best exchange rate for end customers.

The solution requires that a CBDC by design does not leave the jurisdiction to which it belongs, and that the solution is based on a hub-and-spoke model. The hub-and-spoke solution offers higher efficiency than linking many countries' systems together in a one-to-one relationship (in bilateral models).

The report[27] associated with the project, along with a video [28], was released on March 6th, 2023. A description of the hub-and-spoke-model developed during Project *Icebreaker* appears in Figure 6.

[23] As also with small changes in the algorithms can be quantum resistant.

[24] See Norges Bank news report: https://www.norges-bank.no/tema/finansiell-stabilitet/digitale-sentralbankpenger/prosjekt-icebreaker/ and news from BIS: https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm.

[25] The countries have different technologies in use in their PoCs/prototypes - the Riksbank uses Corda, while the Bank of Israel uses Quorum.

[26] Foreign Exchange Providers.

[27] https://www.bis.org/publ/othp61.htm

[28] https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm

As a result of the project, Norges Bank has gained valuable experience and expertise from other central banks' CBDC projects. The project also proved that a technology-agnostic approach could be adopted, implying that each country can employ various technologies in their CBDC-design. The hub will in principle have the capability to collect exchange rates from a large number of FXPs allowing the payer to select the best exchange rate in the market. FXP can be a market participant that offers currency exchange. The selected FXP has holdings of CBDCs in at least two countries' CBDC and is responsible for executing the currency conversion/payment. A technology designated as Hashed Timelock Contract (HTLC) is used, which ensures that money is not compromised and cross-border payments may be completed in seconds.

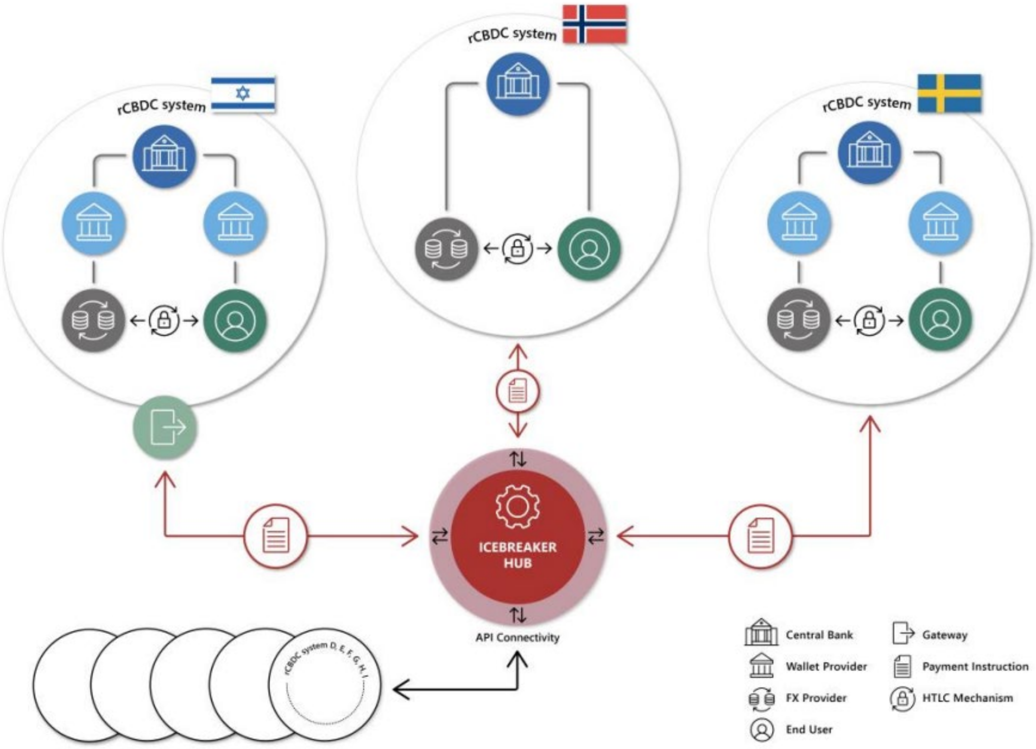


Figure 6 Hub-and-spoke model in Icebreaker

Source: Project *Icebreaker*

The experiment has several implications depending on further policy and technical adjustments. Project *Icebreaker* only explored one way to help streamline cross-border payments via CBDC.

The construction of a hub-and-spoke solution such as this is driven by a desire for a "happy path" (does not test for potential technical problems), without weighing it against other technical solutions offering potentially greater operational efficiency despite high investment in the construction phase.

3.5 Exploring solutions for offline payments

The project did not conduct direct tests of offline solutions. In this context, an offline payment is a CBDC payment that can be made even if it is impossible for both parties to a transaction to communicate with Norges Bank's register at the time of the payment. However, some other projects provided additional information regarding offline solutions during this project.

Two master students at NTNU wrote a master's thesis[29] on design choices for offline solutions pertaining to a Norwegian CBDC. In connection with this, the students conducted a simulation of offline systems, including how sharing transaction data between users can contribute to increasing an offline system's level of security more than if users only store their own transaction history. The students conducted interviews with participants in the CBDC project during their work. This collaboration is a good example of how student projects can supplement validation work.

Project *Polaris* is a project led by the BISIH Nordic Centre whose main purpose is to investigate various CBDC-related offline aspects. Norges Bank is a participating observer in this project.

So far, project *Polaris* has, amongst other things, led to the creation of an offline handbook and a design guide.[30] The handbook addresses key issues in need of clarification in the process of building an offline system.

Among other things, it is important to clarify the purpose of offline payments before designing and building such a system. If contingency is the main purpose, one should define the specific contingency situations that the solution should deal with. For example, is financial inclusion or anonymity of higher importance than contingency? Other important design choices that need to be considered are:

- Whether the system should be based on hardware or software?
- Whether there should be one or several offline systems (and if so, whether these should be interoperable)?
- How will the transfer between the online and offline system occur? Does the money have to be represented in the same way in the two modules? Do users have to transfer part of their CBDC in advance into a separate pocket in their wallet for use when making offline payments?
- When are offline payments final? Can the offline module itself provide finality? Can you make many offline payments one after the other, or do you have to "check in" with the online module between each payment?
- Should restrictions exist on the number or value of payments that can be made offline?

[29] Brekke Espedal, Sjur and Dennis Aleksander Janzso "Design Choices for Offline Transactions in a Norwegian Central Bank Digital Currency". Master's thesis in Communication Technology and Digital Security, Norwegian University of Science and Technology (NTNU), June 2022.

[30] Project Polaris: Part 1. Handbook for offline payments with CBDC. Available here: https://www.bis.org/publ/othp64.htm. Project Polaris: Part 4. High-level design guide for offline payments. Available here: https://www.bis.org/publ/othp79.htm.

4. Collaborative activities that have shed light on the validation work

An overview of important activities in cooperation with partners is provided in Table 3. The activities had several purposes:

- Norges Bank raises the visibility of its CBDC-related work and thereby increases the opportunity for engagement and contributions from a broad spectrum of actors (academia, as well as private and public market participants);
- Methodological activity contributes to an open innovation perspective;
- Established dialogue can be valuable in Norges Bank's further CBDC-related work.

Activity[31]	**Description**	**NB's role**
CBDC project in retail	Project where some large grocery businesses explored use cases for CBDC.	-Observer
Conference & Hackathon in Bergen 21 October 2022 in collaboration with Simula/University of Bergen (UiB)	Conference on CBDC, especially technical aspects. The conference was also the "kick-off" for the hackathon on bridges between registers.	- Co-organiser - Jury member
Brainstorming on 22 November 2022 and hackathon on 19 January 2023 in partnership with Digdir	Norges Bank and Digdir arranged a brainstorming session on 22 November 2022. The start of a hackathon on the same date, which concluded and presented in Norges Bank's auditorium on 19 January 2023. Here several groups presented many interesting use cases.	- Co-organiser
Workshop at the University of Oslo (UiO) 10 January 2023	Technical workshop on CBDC and IoT/M2M at UiO	- Co-organiser
Meetings, events and hackathon in collaboration with Fintech Norway	We have had several meetings with Fintech Norway and Virke. The hackathon was conducted in person in Oslo on 15-17 March 2023.	- Co-organiser

Table 3 Overview of activities

The format of the activities varied depending on the issue and context. Hackathons were used to engage participants in a technical solution, while conferences and workshops were used to attract academics and other target groups, in addition to

[31] Ranked chronologically by start of activity.

providing Norges Bank with valuable information. Brainstorming was essentially centred on a practical aspect.

CBDC project in retail

In autumn and winter 2022-23, the largest grocery-retailers in Norway were owners and participants in the "Central bank digital currency - Use cases in retail" project. Nordic Initiative was the coordinator for the process. Norges Bank was an observer.

The project report[32] stated the motivation behind the project:

> "Being able to buy food is a critical function in society. If CBDCs are to be a true alternative to other forms of payment, they must at least be able to be used to buy food. CBDCs may become legal tender, but even if they are not, grocery merchants may have to accept them. The retail actors should familiarize themselves with the potential implications. But CBDCs may also bring benefits, depending on the features they are equipped with. It is at this point, early in the process, that the opportunities to influence the development of future money are the greatest."

The purpose of the project was to describe and visualise some examples of the use of CBDC in the grocery sector and describe opportunities and challenges. This was to be done in a manner that could be replicated/further developed for other commerce and industries.

The project pointed to some potential benefits of CBDC:

- Increased resilience in the payment system.
- Reduced costs related to the handling of cash.
- Opportunities for innovation, amongst others through the use of smart contracts.

The project also pointed to some prerequisites for a successful implementation:

- CBDC must be sufficiently independent from current payment solutions.
- CBDC must include offline functionality:
  - Opportunities for peer-to-peer payments, for example up to a limited amount.
  - The opportunity to download money to a physical entity.
- The solution should build on principles from blockchain/DLT that allow for smart contracts.
- CBDCs must function well across national borders. It is decisive that central banks work together to ensure interoperability.
- The costs associated with introducing and operating a CBDC must be kept low. It is important that CBDCs do not impose unnecessary costs on merchants or customers. On the contrary, the chosen setup should contribute to increased competition in the payment market.

The project report stated:

> "Through the exploration of central bank digital currencies, the participants have come to the conclusion that the introduction of CBDCs may bring a number of advantages, as long as important prerequisites are met. At the

[32] https://www.nordicinitiative.com/theinitiative

> same time, the retail actors could play a decisive role for a successful introduction. (…).”

For Norges Bank, this was an important activity to better understand merchants’ needs for the payment infrastructure and input to further CBDC-related work.

Conference and Hackathon in Bergen on 21 October 2022 in collaboration with Simula/UiB

The first CBDC conference was held in Bergen in October 2022[33]. The conference was research-oriented with approximately 50 participants from academia, the FinTech community and central banks. International participants such as the BISIH Nordic Centre, Digital Euro Association (DEA) and OpenCBDC[34] also participated. Topics discussed in the conference included: the CBDC-related work at Norges Bank, DeFi and legal issues, AML and CBDC, data protection and CBDC, quantum technology, and OpenCBDC.

The conference became a kick-off for a hackathon[35] focused on transferring CBDC tokens through bridges between openCBDC and EVM-compatible networks. No award was granted for the best contribution in this hackathon.

Brainstorming and hackathon in collaboration with Digdir

In the summer of 2022, work started on planning a brainstorming session together with Digdir. The theme was “Which existing problems can a CBDC solve, and which new opportunities can a CBDC provide to society?” The event was held on Digdir’s premises on 22 November 2022, during which an estimated 100 people attended, who were divided into groups for brainstorming. At the end of the day, the groups’ suggestions were presented in a plenary session. This day also included the start of a technical hackathon. The hackathon was carried out in groups of up to five people that programmed technical solutions in Norges Bank’s prototype/sandbox. 11 groups presented valuable suggestions regarding the advantages of CBDCs during an event at Norges Bank on 19 January 2023.

Workshop at UiO

On 10 January 2023, we conducted a workshop with the Blockchain Lab at the UiO. The university participated with lecturers from the academic community sharing extensive knowledge of various aspects related to blockchain technology such as IT security, environmental protection and processing capacity. A considerable amount of time was also devoted to the IoT and M2M communication and payments.

Meetings, events and hackathon in collaboration with Fintech Norway

The hackathon was targeted at members of Fintech Norway and Virke. The duration of the hackathon was of three days and thus it was the most compact hackathon

[33] Dedicated website for the conference can be found here: https://simula-uib.com/cbdc-event-2022/.

[34] The programme for the conference can be found here: https://simula-uib.com/wp-content/uploads/2022/11/Bergen-CBDC-Conference-programme-v2.pdf.

[35] A dedicated hackathon website can be found here: https://www.cbdc-hack.no/.

organised in this phase. Two groups joined the final presentations that were limited to visualisation through PowerPoint presentations. The activity was successful in engaging private market participants to become more familiar with our prototype. In addition, the broad spectrum of participants provided the opportunity to develop the customer-oriented concepts and underlying technology that can be adopted. Among other elements, the possibility of semi-offline CBDC enabled via DAG technology (the same technology in use as for IOTA) was mentioned. The possibility of peer-to-peer transactions via the escrow vault (which in part uses HTLC mechanisms), potential data protection solutions and improved user experiences were brought up. With the limited time at their disposal, the groups were unable to develop technical solutions.

5. External tests that have enriched the validation work

5.1 Tests conducted by other central banks/BIS

The vast majority of central banks are involved in some form of CBDC-related work.[36] Most of the central banks are considering retail CBDC (rCBDC). Many central banks are also looking at wholesale CBDC (wCBDC) for settlements between banks and large financial market participants. This is to be seen as central bank reserves in tokenised form and could potentially enhance the settlement of trading and payments in tokenised assets. Studies of wCBDC can also provide useful knowledge about the way to design rCBDC. The text below deals with rCBDC.

Currently, only a few central banks in developing countries and emerging economies have introduced a CBDC. Many central banks are investigating CBDCs without having adopted a position regarding an introduction. Several of them have developed various forms of prototypes in order to gain more knowledge about different technological solutions and design choices.

Some topics among central bank studies in advanced economies:

- The focus is on CBDC used for payments and not for store of value. Many central banks are considering limits on amounts and other frictions to support this and avoid adverse consequences associated with large and rapid transfers from deposits in private banks to CBDC.
- Technological platform: The central bank is responsible for core infrastructure and some basic payment solutions. Private (regulated) market participants develop and offer services on top of this infrastructure.
- Many are looking into different token-based solutions, but some are also considering elements of more traditional payment technology.

[36] According to a 2022 BIS survey, 93 per cent of the central banks in a broad sample were engaged in CBDC work in some form. See Kosse and Mattei (2023). Making headway - Results of the 2022 BIS survey on central bank digital currencies and crypto, BIS Papers No 136. Available here: https://www.bis.org/publ/bppdf/bispap136.htm.

- There is a focus on programmability, for example the idea that a predefined event should trigger payment. At the same time, they wish for all CBDCs to be identical for payees and just as unrestrictedly reusable.
- Data protection and privacy is a key issue: CBDC payments should not be anonymous, at least not payments exceeding a certain amount, but central banks and other authorities should not see personal data.
- Development of a scheme with rules for what the central bank permits and prohibits different market participants to do (division of responsibilities and roles).
- Distribution models and the manner in which CBDCs should interact with the rest of the payment ecosystem.
- The cost of basic payments with CBDC for users and how PSPs should be able to charge and have incentives for innovation.

Among central banks in advanced economies investigating CBDC, the Eurosystem appears to be far ahead. In October 2023, the Governing Council of the ECB decided to take the work further in a “digital euro preparation phase”.

The central banks of Sweden, the UK, the US, Canada, Japan, India, Singapore and Australia are other central banks that are assessing CBDCs and developing POCs, prototypes and/or pilots for CBDC solutions. More recently, these central banks have invited financial institutions and other stakeholders in the payment system to reference groups to discuss various aspects of CBDCs of importance to them. In this way, central banks can obtain input that may be important for the successful introduction of CBDC solutions.

International organisations such as the IMF and the BIS are also devoting a lot of resources to analysing various issues related to a CBDC. Several BISIHs have been established to investigate and experiment with how new technology can strengthen the financial system. BISIHs has several projects that affect a CBDC and can provide useful information for our study. Project *Polaris,* that investigated functionality for offline payments, and Project *Icebreaker*, that tested cross-border payments, are described above. Norges Bank is also an observer in Project *mBridge*[37], and has monitored Project *Rosalind*[38]. Project *mBridge* examines a common CBDC infrastructure and cross-border payments for multiple central banks, while Project Rosalind is developing prototypes for APIs[39] for the deployment of CBDCs and test cases for this are discussed.

5.2 Tests conducted by private individuals and organisations

In addition to testing conducted under the auspices of central banks and the BIS, a good deal of testing is also being conducted privately, both by private market participants with commercial interests in CBDC and by organisations without a

[37] https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

[38] https://www.bis.org/publ/othp69.htm

[39] Application Interface Programming (API) is an interface for how two or more computers/IT solutions can communicate with each other. In Rosalind, this applies to communication between the central CBDC register and private payment service providers (PSPs) to general purpose users.

purely commercial purpose. Below are some of the tests conducted under private auspices briefly described. The overview is not exhaustive.

Several organisations have been established representing different interests related to the development of CBDC. In the US, The Digital Dollar Project has[40] issued a number of publications. Similarly, The Digital Pound Foundation exists[41] in the UK. In the EU, The Digital Euro Association (DEA) has[42] been established as a private think tank around both public and private (in the form of stablecoins) variants of a digital euro. Data protection features associated with a digital euro[43] has been an area of focus for DEA, and this work was used in Norges Bank's testing. Gross et al. (2021), which has been utilised in our experimental testing, springs from the environment surrounding the DEA. In connection with Gross et al. (2021)[44], an open source code has been published[45], which among other things can be used to test and validate the experiments with anonymous payments made in Gross et al. (2021). This was carried out as part of the validation work.

Many banks and financial institutions are exploring and conducting tests.
Both Mastercard and Visa have conducted CBDC-related tests. Mastercard has both tested how CBDC can be integrated into Mastercard's payment network and has developed an environment where central banks can test CBDCs.[46] Among other initiatives, Visa, in collaboration with the company Consensys, has developed a solution for connecting CBDC to Visa's payment network.[47] Both Visa and Mastercard have also conducted tests related to integrating blockchain-based solutions, including stablecoins with their payment network. Such tests are also relevant for CBDC based on similar technology.

6. Summary of validation of the characteristics

Below is a summary of the validation of the characteristics to be tested. Table 2 above also indicates which test cases cover which characteristics.

[40] https://digitaldollarproject.org/

[41] https://digitalpoundfoundation.com/

[42] https://home.digital-euro-association.de/en

[43] https://blog.digital-euro-association.de/privacy-and-cbdcs-dea-working-group?hsLang=en

[44] J. Gross, J. Sedlmeir, M. Babel, A. Bechtel and B. Schellinger (2021). Designing a Central Bank Digital Currency with Support for Cash-Like Privacy. Available here: http://dx.doi.org/10.2139/ssrn.3891121.

[45] https://github.com/applied-crypto/cbdc

[46] https://www.mastercard.us/en-us/business/issuers/grow-your-business/crypto/central-bank-digital-currencies.html

[47] https://usa.visa.com/visa-everywhere/blog/bdp/2022/01/13/envisioning-a-future-1642034573970.html

6.1 Claim on Norges Bank

A CBDC shall be a claim on Norges Bank. This means that Norges Bank issues CBDC, and that CBDC is shown as a liabilities item on the central bank's balance sheet on a par with notes and coins as well as central bank reserves.

The characteristic "claim on Norges Bank" primarily pertains to accounting law and as such is not suitable for technical testing. This characteristic is nevertheless essential for CBDC to gain general purpose users' confidence. All testing and validation in the group's work was based on the assumption that Norges Bank issues CBDC, and that these are distributed to banks. Testing revealed that this characteristic does not raise technical problems and can be conducted without difficulty. This applies both to Norges Bank's own prototype and to the other solutions examined by the working group.

If a CBDC is transferred from the blockchain on which Norges Bank has issued a CBDC to another blockchain operated by parties other than Norges Bank, a bridge must be established, as described above. One concern with the use of such bridges is that the identifiers on the other blockchain are not the same as those issued by Norges Bank. Technically, the token issued is different from the one issued by Norges Bank. This token can be called synthetic CBDC. To which extent this type of synthetic CBDC should legally be judged as real CBDC, or as privately issued money, which in this context must be regarded as stablecoins, is a question that must be resolved by legislation. We do not take a position on what is the best solution in this case. We only mention that if synthetic CBDCs are to be equated with genuine CBDCs, then they must still be a claim on the central bank. In the case of the opposite solution, synthetic CBDC will be a claim on the legal entity responsible for conversion from genuine CBDC to the token in question.[48]

6.2 Parity value with cash and bank deposits

CBDC shall have parity of value (1:1) with bank deposits and cash as well as other central bank money (central bank reserves). Unrestricted transfers between CBDC and bank deposits, between CBDC and reserves, and between CBDC and cash are in most cases assumed to be sufficient to ensure parity. In extreme cases, situations may arise in which parity may come under pressure, for example when depositors are uncertain about the financial strength and liquidity of the entire private banking sector. This also applies to cash.

Parity is not a characteristic that is appropriate for direct testing. Parity presupposes unrestricted conversion between different forms of money, but conversion functionality was not part of the test setup during this phase.

[48] This issue is discussed in further detail in Norges Bank Staff Memo 4/2023.

6.3 Customer orientation

CBDC should have a customer orientation. This means, first, that the system should be accessible to a broad public. Second, the system should be attractive enough to ensure adequate use.

To be attractive, it should be possible to use CBDC in several different payment situations, for in-person shopping, for online shopping and for transfers between private individuals. To ensure adequate use, it is probably necessary either for third parties to develop attractive solutions or for the CBDC infrastructure to be linked to existing payment solutions or payment instruments.

In the test phase, a simple user interface was developed that provided access to the prototype. Further development or new development of different types of user interfaces is both possible and feasible. In the test phase, we did not test the connection to existing payment solutions or payment instruments, nor to different payment situations.

Many of the test cases that were conducted were customer-oriented, as emphasis was placed on increased payment system functionality and efficiency. Project *Icebreaker* and tests of mass payments are examples of test cases that can be described as customer-oriented. In addition, contact with various end-user environments through several hackathons focused on customer-oriented solutions.

The tests showed that it is possible to make CBDC available to a broad public. In principle, it is possible for third parties to develop solutions aimed at general purpose users that are attractive enough to ensure adequate use. But whether a Norwegian CBDC, if issued, in fact reaches adequate use depends on banks and other third parties developing efficient and attractive services based on CBDC.

6.4 Adequate frictions in transfers between CBDC and bank deposits

It is reasonable for a CBDC system to be designed so that frictions are possible to limit unwanted transfer volumes from bank deposits to CBDC. This can, among other things, reduce the effects of potential bank runs and contribute to financial stability.

The use of volume limits and (low or negative) interest rates are examples of frictions. The use of interest on CBDC was subject to testing (see test case G above). The use of volume limits was also tested in this phase (see test case I above).

Testing has shown that it is possible to design solutions that can provide sufficient and desired friction against undesirable transfer between bank deposits and CBDC.

6.5 Controlled by Norges Bank

A CBDC system must be controlled by Norges Bank. At minimum, this means that Norges Bank must control the issuance and destruction of CBDC and the fundamental characteristics of the CBDC system.

In the experimental testing, we validated that a CBDC token can be issued within the prototype where Norges Bank has control over issuance and destruction. Only Norges Bank can issue and destroy CBDC. By testing so-called swaps and bridges, we were able to test whether it was possible to move CBDCs between different registers without offering other market participants the opportunity to issue and destroy CBDC. However, it is conceivable that this transfer of CBDC may represent a vulnerability, which may pave the way for unauthorised issuance of CBDC. At worst, this could expose the central bank to substantial economic losses. In addition, such unauthorised issuance and destruction can threaten confidence in the system, as well as raise a number of legal issues related to liability.

If interest is to be paid on CBDC, payment of interest may require issuance of new CBDC. Any calculation and payment of interest on CBDC will have to be fully automated. This may entail that CBDC is issued by a smart contract without the direct involvement of Norges Bank, so that the procedures followed in the ordinary issuance of CBDC are not followed. In our test case on interest, CBDC was issued in this way. The implications for control, including the security challenges associated with this way of paying interest, may need to be assessed further.

In the prototype, we had control over the basic characteristics of the system. The basic characteristics of CBDC tokens were programmed into the contract when CBDC was issued and only Norges Bank could issue the CBDC token. By selecting a closed (private) network, we had control over those who had access in addition to the code used and the validation of transactions.

The use of open source code also raises questions related to control. The code and dependencies in the code are continuously developed by a “community”. Although Norges Bank does not need to make any modifications (latest version) to the code, this may be necessary, partly because of security and interoperability. Such developments may affect the characteristics of the system, thereby meaning that Norges Bank loses some control over its characteristics. Dependence on code developed by third parties and characteristics determined by third parties becomes even clearer if one allows CBDC to be moved to other registers through bridges, especially if one allows CBDC to be moved to privately operated registers. In such cases, one will also be dependent on development plans determined by others. As an example, in one of the test cases, we were dependent on the development of a third party to carry out the test case. The overall conclusion is therefore that the use of open source code raises some challenges in terms of control. Further testing and analysis is conducted to assess whether the use of open source code provides sufficient control.

The starting point for a Norwegian CBDC is that third parties develop applications for the use of CBDC, and thus can fulfil the characteristic of being a platform for innovation. This may conflict with the need for control. Norges Bank can lay down both technological and regulatory guidelines for the applications that third parties can develop and the requirements for application developers. In the prototype, there were basically no restrictions on how users could design digital wallets and send money from one wallet to another. We did not directly test how to place restrictions on creating digital wallets, but the test cases related to digital identity (VC) and KYC make it possible to prevent transactions and owners of CBDC that are not legitimate. Technical and regulatory instruments for maintaining control over who can offer payment services in a CBDC system should be further explored in a next phase to find the adequate trade-offs and mechanisms between control and innovation by third parties.

6.6 Capable of functioning as legal tender

The idea that a CBDC should be able to function as legal tender is primarily a legal characteristic in the sense that a CBDC must be placed on an equal footing in law with notes and coins issued by the central bank. This aspect of the characteristic is not subject to technical testing.

If CBDC is to function as legal tender in practice, a CBDC must nevertheless be required to be easily accessible and in part easy for end-users to pay with in practical situations. Technical testing showed that CBDC can easily be distributed from Norges Bank to banks. Moreover, the testing showed that CBDC can be distributed from banks to end-users' electronic wallets (see test case B above), also in the form of mass payments (see test case D above). Testing therefore showed that CBDC can be readily available to end users (who have appropriate wallets). However, testing of the prototype did not take into account that CBDC payments should be user-friendly for all groups of end-users. On the whole, usability and the customer journey made up a smaller part of the testing. Testing did not therefore fully verify that CBDC as legal tender will function in practice as a user-friendly means of payment. User-friendliness will therefore be a key feature to develop in the next phase of the project.

6.7 Compliant with obligations under EEA law

This characteristic primarily refers to two sets of rules: the AML Regulation and GDPR. Testing of Norges Bank's own prototype has shown that the identity of a CBDC user can be verified by the payee. This has partly been done through a separate identification solution that is added to the token, and partly through the VC solution in collaboration with Digdir. A number of outstanding issues relating to regulatory responsibility for transaction control remain, but it can be assumed that satisfactory identity verification solutions can be established.

Which personal data will be stored using CBDC, where this information will be stored, or which security solutions will be satisfactory has not been yet been decided. Testing of the alias database has shown that information about the owner of a wallet with name, national identity number and mobile phone number can be stored securely, and that incorrect payments can be avoided. The solution with a database (MYSQL) on a server outside the blockchain also means that the customer's bank can carry out customer control measures in accordance with AML legislation.

If citizens of other EEA countries outside of Norway do not have access to payment solutions for CBDC, this could challenge the provisions on the four freedoms in Part II and Part III of the EEA Agreement. Such issues have neither been tested nor assessed. We would nevertheless like to point out that through Project *Icebreaker* we have tested that cross-border CBDC payments can be made.

6.8 Payments are immediate and final

The characteristic related to payments being immediate and final is well tested through the protype. Users of the solution will immediately receive their funds when the transaction is completed, and no intermediary exists when the same register is used. As such, the payment will also be final when it has been validated and the register has been updated. The cryptography used to secure the register will prevent unauthorised alteration and thus ensure that integrity is safeguarded.

The transfer of money from one currency to another has been validated through the use of foreign exchange third parties. Upon payment, the funds will first be locked in the sender's currency. The third party making the exchange will then automatically transfer an amount to the final recipient based on the agreed exchange rate. When the payee receives the amount, at the same time the money from the sender will be released to the third party responsible for conversion. In this context cryptography is also used in the various registers to ensure integrity (finality). The tests in Project *Icebreaker* as discussed above are an example that explains this in detail.

6.9 Compliant with sound IT architecture principles

Compliance with sound IT architecture principles is a comprehensive characteristic. The work on the prototype was driven by needs related to experimental testing, and a number of simplifications were made with regard to a holistic and secure architecture. Nevertheless, the work addressed several areas that are relevant and compliant with sound architectural principles.

Interoperability is an important aspect that was addressed through testing of different types of bridges in order to exchange CBDC with registers and solutions that use a different technology than Norges Bank's prototype. Successful tests were conducted regarding cross-border payments and an IoT network for simulated buying and selling of electricity. In addition, successful tests were conducted concerning the central register for identity (Id-portal). A prerequisite for interoperability is the use of standards with sufficient market penetration. Validation work used standards such as ERC-20, which currently has good market penetration. However, it is important to keep up with developments and, in particular, any choices made by major market participants such as major central banks.

Another important architectural principle is that the solutions should offer a high level of security. This is achieved through security-in-depth, where multiple layers of security ensure increased resilience to unauthorised access and cyberattacks. In the work on the prototype, simplifications were made in this area, and there are a number of measures and improvements that must be implemented before a solution is ready for production. This includes measures to prevent compromise and measures to detect and deal with attempted compromise. The assessment is nevertheless that the basic technology used has the potential to achieve sufficient resilience and security levels with the adequate implementation. The technology is in active use in the market, and security assessments were carried out.

Another aspect related to security is data privacy. In the prototype, the register is available to all participants and everyone can see everything. This means that the register shows all transactions that have been carried out with amounts. The transactions occur between digital wallets that are identified by long strings of text. As such, a direct link to the person who owns the wallets will not exist, but this can be inferred as payments are made. As mentioned, there will also be a balance between privacy and banks' KYC and AML/CFT requirements.

User-friendliness and the "customer journey" are important for the CBDC system's attractiveness, but as mentioned earlier, this was given low priority in the work on the prototype for capacity reasons. In the event of the introduction of a CBDC, it is important that universal design requirements are also met in order to ensure accessibility for people with disabilities, among other things. For example, one can test whether payments with wallets in the prototype are feasible with accessible solutions for people with disabilities.

A number of other aspects related to architectural principles were addressed through the work in Phase 4. The use of open source code and public availability of Norges Bank's source code were instruments for simplifying innovation efforts. This enabled more people to contribute to the work and build on the prototype, for example through hackathons. The approach chosen for the work on the prototype also revealed some weaknesses with regard to operation and management of the solution, including that the register should be reset in the event of certain changes. Greater focus must be placed on operations and management with work on a solution that could potentially be put into production.

Modularity is important for the IT solutions of the future, also for CBDC. The ability to replace poorly functioning components with new ones that function better has not been tested. This may be subject to tests in future work on CBDC.

6.10 Technical independence and possibility of offline payments

The CBDC system should have the capacity to function sufficiently independently of banks' payment systems to ensure contingency arrangements.

The test prototype facilitates transactions directly between end users, without going through banks. The prototype also enables the authorities or Norges Bank to transfer CBDC directly to households or firms (using CBDC digital wallets) in contingency situations where banks' systems are down.

In a full-scale solution, however, there will need to be a stronger connection to other systems, because the conversion and transfer between bank deposits and CBDC is impossible independently of banks' systems and because spending CBDC takes place through other market participants' solutions. A solution where several independent third parties offer solutions for end-users on top of Norges Bank's core infrastructure will be able to ensure contingency preparedness even if the requirement for technical independence is not met in the literal sense. It is also conceivable that Norges Bank itself develops and operates a technically independent minimum solution for end-users to use in special situations. A solution of the sort has not been developed or tested during this phase.

Many aspects of technical independence exist that are inexpedient for direct testing. Independence will to a greater extent be a result of how the system is designed and constructed.

Offline functionality
An offline payment can be defined as a payment directly between end users and their payment instruments in situations where there is no contact between the register or the account system and the user interface. The funds must then be stored locally and the transfer between users will take place at a close distance. Offline payments were not extensively tested and issues related to the characteristic are therefore insufficiently verified through testing. Participants from the VG team participated in workshops with the BISIH Nordic Centre in connection with project *Polaris* in Stockholm where different suppliers of offline solutions were offered the opportunity to present their solutions. This provided Norges Bank with valuable input for further studies on offline functionality. Not least the fact that many different solutions based on completely different technology are being studied. The development of a common standard for offline payments has yet to be reached.

6.11 Customer communications and due diligence is undertaken by third parties

It has been assumed in the project that banks will continue to be responsible for KYC and onboarding of new customers, in the same way as they are currently responsible for the KYC/AML/CFT functions. Performing such functions may entail additional work and additional costs for banks, and a good business model should exist for this. Those that may offer digital wallets and payment services based on CBDC in the future may include other types of market participants than banks, provided adequate authorisation, regulation and monitoring are offered.

Both our own prototype and other central banks’ tests of CBDCs showed that it is possible to design a CBDC architecture that provides satisfactory KYC.

6.12 Flexibility to accommodate different data protection and privacy solutions

It is an objective for a CBDC to be robust to various privacy protection requirements and at the same time be able to fulfil regulatory requirements intended to satisfy compliance and control. Data protection and privacy is an overarching social consideration and CBDC must be in accordance with the trade-offs made by authorities, including in accordance with EU legislation such as the GDPR.

Several of the tests we conducted highlighted the range of opportunities for making payments with a high degree of data protection (up to full anonymity) and at the same time ensuring regulatory compliance. We tested an open source code from the academic literature to conduct anonymous payments[49]. As a test case, we also examined how existing services for anonymisation of payments can be used in our prototype, including how this can be combined with regulatory compliance. Data protection and compliance were also highlighted in the hackathons/ideathons we helped organise. We also tested VC which can be an important component of data protection solutions.

The testing showed that the technology we used in the prototype provides a high degree of robustness for different degrees of privacy/data protection and different schemes for regulatory compliance.

Regardless of the starting point, it is important to find technical solutions that are flexible for different requirements and wishes both now and in the future. The needs of society are changing, and new technologies provide new opportunities.

Through the tests that were conducted, we showed that it is possible to achieve flexibility for different data protection solutions.

6.13 Platform for third-party providers/innovation

In several reports (Norges Bank Papers, 2/2019 and 1/2021), this characteristic is discussed as an important innovation prerequisite for CBDC. Several exercises in this phase indicated that the prototype/sandbox can be used as a platform for third-party providers.

This was revealed in the hackathon with Digdir (part 2). 11 groups that were registered had developed innovative solutions (test cases) in our sandbox/prototype. These test cases were presented by a broad spectrum of private and public market participants. In various dimensions, test cases demonstrated how third-party providers can provide services and products to society by integrating their offer with the CBDC prototype. In a case, the offline capability of CBDC was tested for. In other test cases, CBDC functioned as a means of settlement (examples: solutions for the real-time ownership management via smart contracts, payments for temporary workers in Norway, digital wallets in the context of several other test cases, and a solution for settlement in a game developed). In addition, there were examples for solutions “on top of” CBDCs such as personalising CBDCs, using M2M technology, and raising climate awareness.

Interoperability is an important prerequisite for facilitating innovations. Interoperability was tested in multiple tracks during this phase. The testing of a bridge in in test case C is an example of this. Another example is Project *Icebreaker*.

In the testing work in this phase, emphasis was placed on testing the scope of possibilities regarding CBDC’s ability to constitute a platform for third-party providers. In future work on testing, emphasis should also be placed on business models and regulatory framework conditions that offer third-parties incentives for such development.

[49] Gross et al. (2021).

6.14 Safeguard monetary policy efficacy

In addition to the experimental testing described here, separate analytical work was also carried out in the sub-project “CBDC - Consequences for liquidity management and monetary policy”, see Bernhardsen and Kloster (2023)**.**

In the experimental testing we tested through programmability interest rates and amount limits that can contribute to restricting the CBDC’s scope enough to safeguard monetary policy efficacy.

6.15 Information relevant to Norges Bank’s macroeconomic monitoring

In the current CBDC prototypes, it is possible to track transactions in real time, while at the same time being able to access transaction history. Nevertheless, until now multiple roles have not been defined as regards different users (i.e. all users have the same rights, except Norges Bank). If market participants are assigned different roles in the system, enabling the analysis of user patterns, a CBDC has the capacity to provide additional macroeconomic information. This can potentially be included in additional testing work.

With macroeconomic monitoring in this context, safeguarding data protection is a prerequisite. A separate off-chain database with private information has been tested showing the ability to connect the current register (with an alias) with a public register (with an alias-linked ID). Such decoupling of information can enable data protection in macroeconomic monitoring. Various cryptography techniques can also be used to prevent CBDC used in the macroeconomic monitoring from disclosing personal data. This can potentially be tested further.

6.16 DLT compatible

The prototype we have tested is based on distributed ledger technology (DLT) and is thus inherently DLT-compatible. The use of various elements of DLT technology is a hallmark of testing CBDC systems around the world.

The use of DLT in the prototype also makes it partially compatible with other DLT-based systems. This is made possible, among other things, by the fact that the CBDC in the prototype can be locked in a HTLC so that it can only be unlocked if certain conditions are fulfilled. This has been used in so-called bridges in order to transfer CBDCs between different registers and was also central to implementing the test for cross-border CBDC payment systems (Project *Icebreaker*).

The use of DLT should also be central to further testing work, partly because this is central to so-called tokenisation. For Norges Bank project phase 4, DLT capabilities were a prerequisite for participation in Project *Icebreaker*, mentioned earlier. It is also conceivable that DLT-compatibility will be a prerequisite for interoperability between an eventual Norwegian CBDC and other countries’ CBDCs.

6.17 Attractive niche solution

CBDC should also function as a niche solution, i.e., satisfy special payment needs of users.

During this phase, functionality for mass payments was developed and tested. Relevant test cases for this type of mass payment can be payments from public market participants such as tax authorities and NAV.

Project *Icebreaker* was another test case that can be considered as a niche solution, documenting cross-border payments that could be conducted more swiftly, inexpensively and appropriately than current solutions have the capacity to.

Other niche solutions that were not tested could be atomic transactions such as “delivery versus payment” (DvP) in the form of a payment that is completed automatically when an agreed event occurs.

7. Summary and the way forward

Summary
The overall assessment of the project team is that the experimental testing phase was successful, given the time and resources available during this phase of the project. Through experimental testing, we were able to shed light on how technical solutions can fulfil the characteristics of a CBDC. The test work also cast light on necessary trade-offs. For example, Norges Bank’s need for control may limit private market participants’ ability to develop innovative solutions. The experimental testing also elucidated legal, economic and regulatory aspects. Among other elements, different ways of organising so-called bridges have implications for how a CBDC can continue to be a claim on Norges Bank. Through many of the test cases, we only partially validated how the technologies can fulfil the characteristics. Continued testing is therefore necessary in order to provide a better factual basis for decision-making regarding a final recommendation.

Limitations of testing
Testing the scope of possibilities for technology was the theme of the experimental testing. This implies that the tests have been conducted on a limited scale in “simplified” infrastructures. This entails that, among other things, so-called performance testing was not conducted of, for example, capacity limits. Furthermore, a “happy path” was assumed, in which weight was not given to having adequate solutions that take into account intentional or unintentional use of the technology. The prototypes were not developed for the purpose of meeting necessary security requirements of a CBDC system either.

Integration with existing infrastructure
At the start of the fourth phase, it was decided to let the prototype/sandbox be a stand-alone solution. As a result, banks receiving CBDCs in a two-tier architecture by drawing on central bank reserves, as may be the case in production, was not tested. Nor were participating banks requested to enable bank customers to obtain CBDC through withdrawals from their deposit accounts.

Regulations, incentive structures, and business models for third party participation in the system and related tests were not developed either. For example, whether banks or other market participants can be incentivised to participate by receiving a share of fees or something similar was not tested. This can be done during the next phase. This entails that test cases examining various incentive structures should be developed in the next phase.

The experimental testing did not include testing of a holistic infrastructure that can be used for CBDC in Norway. However, the experimental testing shed further light on the potential aspect of a holistic architecture.

A lesson learned from testing is that different registers possess diverse characteristics that to varying degrees can deliver the characteristics required of a CBDC. For example, an account-based solution, such as in Hyperledger Besu and ERC-20 tokens, has adequate prerequisites to offer programmability. Programmability was essential to conducting several of the test cases and was also central to many cases that were developed in connection with the brainstorming/hackathon. So-called UTXO token solutions offer higher efficiency for applications that do not require programmable money or that solely require limited programming functions.

Another lesson learned was that the use of Ethereum technology like Hyperledger Besu attracts more innovation and original solutions, especially in an experimental test, since in Norway and internationally there are a large number of programmers with appreciable experience and expertise.

Different register solutions can therefore present various advantages and disadvantages in several dimensions:

1. Representation of money
2. Programmability
3. Division of roles and decentralisation

Bridges entail that a CBDC is transferred from one register to another separate register. This can be included as a “side-chain”. An alternative to side-chains is to use L2, which means that a new register is placed over the CBDC core register. One possibility with a L2 is that it can be linked more closely to the core register and it may be easier to repurpose some of the security already existing in the core register. L2 and side-chains are not mutually exclusive, and a fluid boundary separating them may occasionally exist. Both bridges and L2 could potentially be tested further in the next phase.

The way forward
The purpose and plan for the fifth phase are explained in the *Norges Bank Papers* 2/2023 with the final report from the fourth phase.

Norges Bank
Norges Bank Papers

Oslo 2023

Visiting address: Bankplassen 2
Mailing address: P.O. Box 1179
Sentrum, 0107 Oslo, Norway
Telephone: +47 22 31 60 00
E-mail: post@norges-bank.no
www.norges-bank.no

ISSN 1894-0277 (online)
ISBN 978-82-8379-294-2 (online)