BIS Innovation Hub

Project Polaris

Part 1: A handbook for offline payments with CBDC

May 2023

Preface: How to read this handbook

For a general overview:

Read the chapters for the executive summary, introduction and offline payments with CBDC.

For more technical details:

Read the chapters for offline payment solutions for CBDC, risk management by design, privacy by design, inclusion by design and resilience by design.

For further technical and operational questions and considerations:

Read Annex A, which provides a set of questions and considerations that could be useful when planning and designing the technology and operations for CBDC systems that support offline payments.

For other details:

Read Annex B. which contains the results of the BIS Innovation Hub survey on offline CBDC payments, and Annex C, which contains a short history on offline payments.

This handbook was developed in partnership with:

Publication date: May 2023

Contents

Acronyms, abbreviations and definitions

Acceptance device	Any point-of-sale device, digital application, e-commerce platform or other solution at an Unattended Merchant Location used to effect a financial transaction.
Accounted system	A mechanism where every transaction is recorded and transactions are not regarded as final until this recording is done.
AML	Anti-money laundering
Authentication	The process or action of verifying the identity of a user, process or system.
Bidirectional protocol	A communications mode that transmits data in both directions (sends and receives), but not necessarily at the same time.
Blinding	A cryptographic technique for disguising the content of a message before it is cryptographically signed. Blinding methods are privacy-protecting and are often used in applications where the privacy of the sender needs to be maintained.
BLE	Bluetooth low energy
Block list	A list of user devices that should not be transacted with, usually because they are suspected of being fraudulent in some way.
Bounty	A payment that software companies make to ethical hackers who identify and report vulnerabilities in their software.
Cash out	Converting CBDC value into another form, such as moving it to a normal bank account.
Cash resemblance	Certain features and aspects of the user experience of using cash that could apply to CBDC.
CBDC	Central bank digital currency
Certificate	Also known as a public key certificate, used to cryptographically link ownership of a public key to the entity that owns it. Digital certificates are for sharing public keys to be used for encryption and authentication.
Chip & PIN	A way of paying for goods by debit or credit card whereby one enters one's PIN into an electronic device (for example, a point-of-sale device) rather than signing a slip. Commonly used to refer to the EMV value transfer protocol.
Clearing	Denotes all activities from the time a commitment is made for a transaction until it is settled.
Clone	The action of replicating data, software or hardware devices, usually in order to create a counterfeited copy of them. This can apply to purses or value-forms.
Counterfeit	Made in imitation of something of value or important with the intention to deceive or defraud
Crypto-agility	The ability of a cryptographic system to adjust to new cryptographic methods or key lengths.
Cryptanalysis	The study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. Often used to refer to the process of accessing encrypted data without knowing the decryption key.
Crypto-durability	The length of time a cryptographic algorithm and/or key length is expected to be resistant to an attack.
Cryptocurrency	A digital currency in which transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralised authority.
Cryptographic key	A piece of information, usually a sequence of numbers, letters or symbols, used in encryption and decryption processes within cryptographic algorithms. It serves as a secret parameter that controls the transformation of plaintext (unencrypted data) into ciphertext (encrypted data) and vice versa. The security of encrypted data relies on the strength and secrecy of the key.

Cryptography	Secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms and used to transform messages in ways that are hard to decipher.
CVM	Cardholder verification method – a mechanism by which the cardholder proves that they are the rightful user of the card. Often implemented using a PIN or biometric.
Digital inclusion	The effort to ensure that every individual and community has access to Information and Communication Technology (ICT), along with the skills to make use of it.
Double-spending	The act of sending a transaction containing inputs that have already been spent in an attempt to commit fraud on the network.
EMV	Europay, Mastercard and Visa – the standard governing the majority of payment cards globally.
Financial inclusion	An effort to make everyday financial services available to more of the world's population at a reasonable cost.
Floor limit	Also known as a "credit floor", the maximum charge that can be made to a payment product without obtaining prior authorisation. Often implemented in PoS devices to limit the value of offline transactions.
Form factor	Main appearance of user device.
Friendly fraud	Fraud perpetrated by or on behalf of the user.
Fully offline system	System in which the payer and payee do not need to connect to a ledger system (though there could be a local on-device ledger) to complete a payment, and any value exchanged is immediately transferred to the payee such that they can spend it at the end of the value transfer (settlement occurs offline). Both payer and payee can stay fully offline without limitation in time.
Global Platform standards	A set of technical standards that allows international industries to share information, developments, methods of payment, etc without being limited by different national systems. Particularly focused on secure elements, smartcards and TEEs.
Hardware-based security	Hardware-based security protects an endpoint from malicious threats by relying on a specific hardware components (or devices). Endpoint software relies on these hardware components to oppose any alteration or tampering.
Hardware security module (HSM)	Devices which hold and process cryptographic keys securely, usually located in secure processing centres.
Hybrid banknote	A banknote that is linked to some form of digital representation such that if the note is spent digitally the physical note becomes worthless.
Integrated circuit card (ICC)	In the context of payments, usually a card with a secure element.
Instant payment system	A system where the value is instantly transferred to the payee.
Intermittently offline system	Similar to fully offline, a system in which the payer and payee do not need to connect to a ledger system to complete a payment, and any value exchanged is immediately transferred to the payee such that they can spend it at the end of the value transfer (settlement occurs offline). However, risk parameters will at some point limit the ability of purses to transact and a purse will have to synchronise with the central system intermittently in order to continue to function.
IoT	Internet of Things
Jailbreaking (a device)	Modifying a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, eg to allow the installation of unauthorised software.
Key fob	A small security hardware device, typically with built-in authentication used to control and secure access to mobile devices, computer systems, network services and data. Key fobs can also be used for contactless payments.
KYB	Know Your Business
KYC	Know Your Customer

Ledger	A collection of financial accounts of a particular type. For CBDC payments, this is the collection of transactions performed by users using CBDC value.
Ledger system	A system or set of systems hosting ledgers. The term specifically does not imply the use of any particular type of technology.
Life cycle management	The process of managing the life cycle of a product. For CBDC purses, this will mean managing the various stages the purse may go through, including processes around re-issuance.
Logical architecture	The organisation of the subsystems, software classes and layers that make up the complete system. Does not necessarily represent physical components.
Mitigation (of risk)	Reducing risks or effects. In the context of cyber security, reducing the risk or effect of a cyber attack.
Mutual authentication	Also called two-way authentication, a process or technology in which both entities in a communications link authenticate each other. For example, in a network environment, the client authenticates the server and the server verifies the client before data can be exchanged.
NFC	Near-field communication
Offline	Not controlled by or directly connected to a computer or external network. For CBDC, this refers to being disconnected from CBDC ledger systems, not necessarily disconnected from communication networks.
Offline CBDC system	A payment app or card-based payment system offered by the central bank that would not require a continuous connection to CBDC ledger systems.
Offline data authentication (ODA)	A mechanism in card payments that allows terminals to authenticate payment cards in the absence of a connection to the payment network.
Offline payment	A transfer of value between devices that takes place without requiring connection to any ledger system.
Offline PIN	Usually a cardholder verification method for EMV chip cards. These cards store the PIN securely on the chip itself, so cardholder verification can occur even on a stand-alone device not connected to a network.
Online PIN	Works by sending an online authorisation message which carries PIN data entered by the Card Member at the Point of Sale (POS) to the Issuer.
Onward spend	The ability to immediately spend received value as opposed to needing to connect to a ledger system to settle the payment first.
Originator	The entity (payer or payee) that starts the payment transaction.
P2B payments	Person-to-business payments
P2G payments	Person-to-government payments
P2P payments	Peer-to-peer payments, usually used to refer to payments between two individuals.
Payment instruction	A message exchanged between two parties indicating the transfer of value.
Payment service provider (PSP)	Offers merchants the support they need to access electronic payments, including credit cards, digital wallets and more.
Personalisation	The process of including data and keys that are "personal" to a specific purse, usually through some secure loading process.
Physical attack	When a threat actor tries to access systems, data, or networks by attacking the physical devices and components that make up the system.
Physical unclonable function (PUF)	A unique, hardware-based feature of a device which guarantees the individuality of the device itself.
Private key	A secret piece of information, usually a sequence of numbers, letters or symbols, used in asymmetric public key cryptography to decrypt messages encrypted with the corresponding public key or to sign digital messages. In an asymmetric key pair, the private key is kept confidential by its owner, while the public key can be freely shared.
Pseudonymity	A process of using a fictional persona to conduct activity without revealing one's true identity.
Public key cryptography	Also known as asymmetric cryptography, the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a

	corresponding private key. These can be used to sign messages, among other use cases.
Purse	A piece of software in the user device which provides the offline payment functionality. This will usually contain data and cryptographic keys specific to that user. This term is used specifically for offline payment functionality.
Quantum resistant cryptography	Quantum-resistant cryptography, also called quantum-resistant encryption or post-quantum cryptography, applies encryption algorithms that should resist to attacks based on quantum computers.
Replay attack	A security breach in which data are stored, re-sent and accepted. For instance, replaying a payment instruction would see the message copied and re-sent. The payee device should reject replayed messages.
Reverse engineering	Reverse engineering is any experimental of deductive process that can be used to infer knowledge about the internal operation of a black box.
Rooting (a device)	The process of unlocking or jailbreaking a device such as a smartphone or tablet.
Scalability	The ability of a computing process to be replicated in many instances across a server network, in order to improve performance and/or reliability.
Secure element (SE)	A chip that is, by design, protected from unauthorised access and used to run a limited set of applications as well as store confidential and cryptographic data. A form of ICC.
Secure enclave	See "trusted execution environment".
Secure hardware	A system which is trusted to perform secure computation processes (ie payments) by the use of secure elements and verified software.
Secure processing centre	A secure site hosting server systems, with specific physical and operational security to make it hard to access.
Side-channel attack	A security exploit that aims to gather information from or influence the program execution of a system by measuring or exploiting indirect effects of the system or its hardware rather than targeting the program or its code directly.
SIM card	A smartcard inside a mobile phone that carries an identification number unique to the owner, stores personal data and prevents operation if removed. SIM cards may be secure elements.
Smartcard	A plastic card with a built-in microprocessor (ICC), typically used for electronic processes such as financial transactions and personal identification.
Social inclusion	The process by which efforts are made to ensure equal opportunities – that everyone, regardless of their background, can achieve their full potential in life.
Software-based security	Software-based security protects an endpoint from malicious threats by relying only on software features. Opposed to hardware-based security, which involves specific hardware components.
Staged offline	Where the payer and payee do not need to connect to a ledger system in order to exchange value, but the value exchanged is not finally settled on the payee until the payee connects to the ledger system. Value transferred to the payee cannot be spent until this second stage of online settlement has occurred.
Stress test	A software testing activity that determines the robustness of software by testing beyond the limits of normal operation.
Store-and-forward system	A data communication method that allows intermediary devices to store messages before forwarding them towards their destination.
Stored-value system	A payment system where value is pre-loaded onto a payment instrument such that it can only be spent using that payment instrument.
Tamper-proof	The capability of any object to resist attempts to modify it. Detection of tampered data is possible by storing their hash function along them, as even small modifications in the original data result in different values of their hash.
Tamper-resistant device	A device that is deliberately hardened to make it difficult for threat actors to expose the contents.
Thin data channel	A data communication channel carrying limited amounts of data.
Threat actor	A threat actor such as a nation-state, organised crime group, hacker(s) or individuals motivated by financial gain. These threat actors could work independently or together.

Trusted execution environment (TEE)	Also known as a secure enclave, a computing environment that provides isolation for code and data from the operating system either by using hardware-based isolation or by isolating an entire virtual machine.
Unaccounted	In the context of offline payments, a transaction that is not shown on any ledger.
Unidirectional protocol	A protocol that does not require a response from the counterparty.
Untraceable transaction	A transaction that cannot be traced to the users involved in it.
User device	A device in the possession of the user which enables them to make offline payments. This could be a smartphone, a smartcard, a key fob, a feature phone or some other piece of technology that provides them with the means to make an offline payment.
Unstructured Supplementary Service Data (USSD)	A data channel provided by mobile phone networks. This is a thin data channel, usually used to communicate small amounts of data, but which allows bidirectional communications.
Value-form	A representation of value held in a purse. For instance, this could be a plain balance (account) or a cryptographically computed digital coin (token).
Value transfer mechanism	Any system, mechanism or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form.
Value transfer protocol	A protocol designed to transport value between two different endpoints (either online or offline). An offline value transfer operates between two hardware devices.
Velocity of transactions	The number of transactions performed in a specified period of time, also cumulative amount transacted over the same period.
Wallet	Any mechanism that can be used to store digital assets (tokens). A cold wallet is a hardware device and can be operated offline, while a hot wallet is an online service based on web resources (and can be operated only by online users).
White-box solution	A subsystem whose internals can be viewed but usually not altered.

1 Executive summary

1. Executive summary

This handbook provides a comprehensive overview of the key aspects of offline payments with CBDC and is intended to serve as a guide for central banks considering implementing offline payments capabilities. In this handbook, an offline payment is defined as a transfer of value (CBDC) between devices that takes place without requiring connection to any ledger system. This could be due to a system outage or in the absence of internet or telecommunications connectivity.

A survey conducted by the BIS Innovation Hub as part of the development of this handbook shows that 49% of central banks surveyed consider offline payments with retail CBDC to be vital, while another 49% deemed it to be advantageous.

Providing offline payments with CBDC is an important requirement for many central banks, but its implementation is complex and involves a number of technology, security and operational considerations that need to be planned and designed for at the earliest possible stages.

These considerations have implications on decisions related to policy, ecosystem roles and responsibilities, design, architecture, security, technology, investment, ongoing operations, change management and risk management.

The research for this handbook has found there is no one-size-fits-all solution, with each country having multiple reasons for providing offline payments with CBDC. The types and suitability of solutions for offline payments will vary by country depending on local requirements.

This handbook provides some of the main reasons and usage scenarios for offline payments; a map and an explanation of the technology components; and a set of design criteria for risk management, privacy, inclusion and resilience. It also provides a set of considerations that central banks can use to inform their planning, policy development, technology and business requirements, procurement activities and future operations.

This handbook is intended to help central banks to:

- understand the available technologies and security measures;
- understand the main threats, risks and risk management measures;
- understand the privacy issues, inclusion needs and resilience options;
- understand the design and architecture principles involved; and
- gain perspective on potential operational and change management issues.

The information contained in this handbook has been compiled from information gathered from expert advisers, the survey of central banks, interviews with private-sector companies, meetings with central bank experts and other research.

Key takeaways

Policy and design

- Providing offline payments functionality with CBDC could be a way for a central bank to achieve a broad set of public policy objectives, including those related to its mandate. A central bank should identify how offline payments with CBDC could support relevant policy objectives, such as inclusion or payment system resilience.
- A central bank should also consider its risk tolerance and approach to risk management, how to handle cases of lost value, and the balance between privacy objectives and those for AML/CFT.
- The roles and responsibilities of the actors involved in a CBDC payments ecosystem in supporting offline payments should be clearly defined. Collaboration between the public and private sector would be necessary.

Technology, risk and security

- A risk-based approach must be taken at the earliest stages of designing the technology and business operations for CBDC systems, particularly if supporting offline payment, due to possible security and operational implications. This may require adaptation of enterprise risk management to new threats and risks.
- Offline payment solutions can operate in three modes,[1] which refer to how the solution would connect online if and when required. This could have implications for how risks are managed, the level and type of privacy provided, and the resilience conditions that are supported.
- Offline payment solutions can be based on tamper-resistant hardware, software or a combination of both hardware and software (hybrid).
- In some countries, software-based solutions will be more appropriate than hardware-based ones, or vice versa. The type of solution and the mode in which it operates will determine its suitability in meeting various objectives for providing offline payments with CBDC. There is no one-size-fits-all solution.
- Where possible, existing technologies and infrastructure should be leveraged to enable offline payments with CBDC; however, any solution should adapt to new requirements and leverage new technologies over time.

Public service and user experience

- Capabilities for offline payment with CBDC should be provided as a public service for resilience reasons, even if the number of use cases decreases over time, for example due to improvements in internet or telecommunications connectivity.
- Everyday users will demand solutions that are reliable, easy to use, convenient, and widely accepted and that provide a seamless user experience both online and offline.

---

[1] The three modes of operation are fully offline, intermittently offline and staged offline. These are discussed in more detail in Chapter 2.

2 Introduction

2. Introduction

The ability to make offline payments with CBDC has attracted increased interest among central banks as investigation into, exploration of and expectations for CBDC have developed. Many central banks view offline capability as a potential way to achieve other objectives such as financial inclusion, universal access, payment system resilience and privacy.

Implementing offline functionality is complex, involving a number of technology, security and operational considerations that need to be planned and designed for at the earliest possible stages due to their implications on policy, design, implementation, operations and risk management. It is important to note that not all risks can be fully eliminated, but they can be mitigated using a combination of technical and non-technical measures.

An offline payment with CBDC is defined as a transfer of retail CBDC value between devices that does not require connection to any ledger system, often in the absence of internet or telecoms connectivity.

The handbook contains the following chapters:

Chapter 3: Offline payments with CBDC

Central banks may have a wide range of reasons for introducing offline CBDC, which are described in this section along with a classification of the various types of offline payment system that are available in the market. Offline payment systems can vary in a number of ways, most notably in terms of when and how payments are made available to the payee for further use.

Chapter 4: Offline payment solutions for CBDC

There are many offline payment solutions available from the private sector. This section presents a logical architecture with the main components of an offline payment system and discusses the differences and trade-offs between available solutions.

Chapter 5: Risk management by design

A risk-based approach must be taken at the earliest stages of designing the technology and business operations supporting CBDC systems. Risk management by design would cover technology, operational and reputational aspects. This is key to ensuring trust in CBDC as a monetary and payment system, since trust will be an important objective for central banks that choose to move forward with their CBDC projects.

Offline payments present new risks, including the possibility of CBDC value being counterfeited, lost or temporarily made unavailable. This section discusses both the main risks presented and some possible countermeasures available to mitigate them.

Chapter 6: Privacy by design

Privacy is seen as a key requirement for CBDC payments. However, offline payments present different privacy issues as they can both support anonymous transactions and be privacy-revealing depending on design. This section discusses the main privacy principles and considerations and their application to offline CBDC payments.

Chapter 7: Inclusion by design

Inclusion is an important requirement in order for CBDC payments to be seen as a public good. Offline payments can improve the inclusivity of a CBDC system if designed well, but they could also reduce inclusivity if they limit user access by introducing restrictions on how the offline CBDC can be used or if the solutions or devices are unsuitable for certain situations.

Chapter 8: Resilience by design

Offline payments with CBDC could improve the resilience of a payment system, but only if the design is appropriate to the required resilience scenarios and there is sufficient planning of the infrastructure to support it. This section discusses the different types of resilience scenario, one or more of which will apply differently in each country.

The document also contains the following annexes:

Annex A: Further questions and considerations

An extended list of additional considerations that should be taken into account by central banks planning to issue offline CBDC.

Annex B: BIS survey of central banks on offline payments with CBDC

A summary of the answers provided by central banks in response to the survey undertaken by the BISIH Nordic Centre in conjunction with this document.

Annex C: A brief history of offline payments

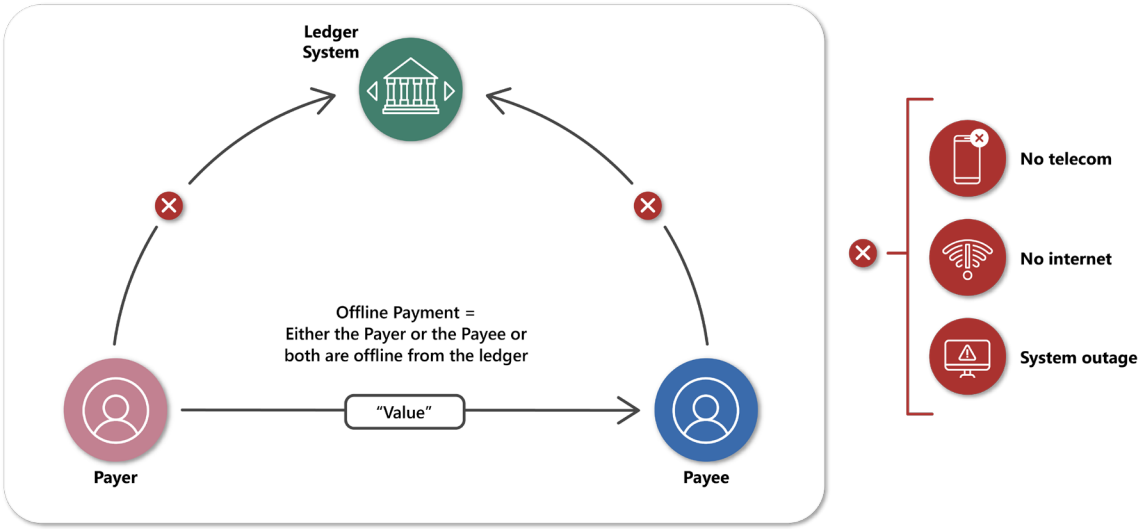
An extended description of a range of examples of offline payment systems that have been previously deployed and an examination of the lessons that they can offer for future offline CBDC systems.

3 Offline payments with CBDC

3. Offline payments with CBDC

In this handbook, an **offline payment with CBDC** is defined as a transfer of value (retail CBDC) between devices that does not require connection to any ledger system, often in the absence of internet or telecoms connectivity. Note that a user device may be online (connected to the internet), but still disconnected from a ledger system.

Offline payments and ledger systems — Figure 1



3.1 Reasons for offline payments with CBDC

There are a variety of reasons why offline payments with CBDC might be needed.

In the survey on offline payments with CBDC conducted in conjunction with the development of this handbook, central banks stated that their primary goals for providing this were financial inclusion, resilience and cash resemblance. Some central banks also cited specific local reasons, for example regions of low network connectivity or provision for disaster recovery.

The following list describes the motivations central banks cited in the survey for providing the ability to pay offline with CBDC:

1. **Resilience**. Use of digital payments is increasing and, in many countries, has become individuals' preferred way to pay.[2] This has created a greater dependency on digital payment systems provided by private and public-sector entities (for example, clearing or settlement services for instant payments).

[2] See Glowka et al (2023).

Availability issues with digital payment systems, for either major or minor reasons, may leave both individuals and businesses exposed and unable to pay or receive payment. It is important to make sure that the overall payment system is resilient at all times.

CBDC systems would face the same challenge, but the ability to pay offline could enable the system to operate for a period of time without connectivity, providing a layer of resilience.[3] The type of resilience scenario and the duration of an outage will have implications on the design of the system, the solutions used, and operations.

2. **Cash resemblance**. Offline payments with CBDC could offer some of the user experience and features of physical cash payments, but in the digital space. For example, funds could be loaded into a digital wallet[4] from an ATM in almost the same manner as we load notes into a physical wallet. However, some features of cash, such as anonymity, may not be fully achievable in practice.

3. **Inclusion**. Most central banks have a requirement for CBDC to support inclusion, or the ability of all of society to use CBDC for payments. Inclusion is broader than financial inclusion and extends to social and digital inclusion. For example, where individuals are unable to access payments using mainstream options such as smartphones or an internet connection, alternatives should be available.

4. **Lack of developed communications infrastructure**. There are many parts of the world, both in advanced economies and in emerging market and developing economies, where internet or network connectivity is unavailable or unreliable.

5. **Privacy**. Offline payments are sometimes perceived as the CBDC use case similar to present-day use of cash, which offers a level of privacy and anonymity. As offline payments with CBDC would typically be disconnected from a ledger system, it technically would be possible to offer more privacy than with online payments with CBDC. However, this would need to be balanced with AML/CFT and KYC/KYB requirements. In the survey, 44% of central banks answered that the level of privacy for offline payments with CBDC privacy should be greater than for online payments. 56% answered that it should be the same as for online payments with CBDC, while no central banks felt it should be lower.

6. **Lower transaction costs**. CBDC systems could help promote competition and potentially lower costs to businesses. Offline payments could potentially incur lower transaction costs than online systems[5] and may allow CBDC systems to target use cases that involve small transaction values. However, this would require consideration of the implementation and operational costs of maintaining and upgrading the supporting offline infrastructure (especially from a security

---

3 Sveriges Riksbank (2022).

4 In this handbook, the term purse is used specifically in the context of offline payment functionality. In practice, some digital wallets could support offline payments.

5 Messages do not need to be sent to the central component for each payment, as payment information can be "batched" and sent to the central component in an off-peak period, which saves time and costs.

perspective), as well as the cost of acquiring and distributing user devices and merchant point-of-sale terminals.

7. **Performance and scalability support**. Offline payments could reduce the overall load on ledger systems. For example, if CBDC systems support use cases that could allow for very small transactions, eg micropayments, then the potential volume of transactions and the scalability required could be greater than what is required today. Offline payments, ie transacting outside ledger systems and providing an alternative processing route, could be an option to support scalability needs.

   However, this would depend on the type of solution and overall system architecture because the size of data downloads (as a result of transaction history volume and the latency window between settlement and synchronisation with the central ledger) could potentially hinder performance and impede scalability.

8. **Universal access.** In many countries, cash is the only form of payment with universal access. Where cash use is declining, legislators are increasingly considering mandating that financial institutions guarantee access to cash.[6] A principle of universal access may uphold public trust in the usage of CBDC, provide freedom of choice and support inclusion aims by preventing certain groups of society or unbanked people from being disadvantaged. In the survey, 53% of central banks said that merchants should accept offline CBDC if they accept online CBDC.

9. **Civil contingency.** There are a range of situations that could make established infrastructure and network connectivity unavailable for a prolonged period of time, such as cyber attacks, natural disasters or conflicts. In these civil contingency scenarios, the ability to pay with CBDC when offline could allow the payments ecosystem to continue to function where other electronic payment methods would be unable to operate.[7]

10. **Trust.** Supporting an offline payment capability could foster citizens' trust in the CBDC system as a whole if it works whenever and wherever they need it to, whether online or offline, and therefore can be trusted to be reliable and available.

11. **Making digital peer-to-peer (P2P) and person-to-business (P2B) payments.** People may exchange value among themselves and with businesses in the same way they currently do with cash, with minimum intervention by a third party.

---

6 See, for instance, European Central Bank (2020).

7 There would be limitations to this, as several solutions would only work for a certain amount of time due to device capacity, power or the need to connect back online periodically. Certain types of solutions may be better suited to this purpose than others, and ultimately cash may be a more suitable contingency option, though distribution and circulation could be a challenge. Offline payment solutions could be complementary to cash, depending on the contingency event.

3.2 Modes of offline payment

This section introduces the three different modes[8] of offline payment.

Before these modes are discussed, it is important to clarify that settlement is the discharge of a financial obligation and, in the context of offline payments, refers to the transfer of funds between the payer and the payee.[9]

Solutions providing offline payments functionality can be categorised as follows:

- **Fully offline:** Where the payer and payee do not need to connect to a ledger system to complete a payment, and any value exchanged is immediately transferred to the payee such that they can spend it at the end of the value transfer (final settlement occurs offline). Both payer and payee can stay fully offline without limitation in time.
- **Intermittently offline:** Like fully offline, the payer and payee do not need to connect to a ledger system to complete a payment, and any value exchanged is immediately transferred to the payee such that they can spend it at the end of the value transfer (final settlement occurs offline). However, offline risk parameters could at some point limit the ability of purses to transact and a purse may have to synchronise with the central system intermittently in order to continue to function.
- **Staged offline:** Where the payer and payee do not need to connect to a ledger system in order to exchange value, but the value exchanged is not settled on the payee until the payee connects to the ledger system (final settlement occurs online). Value transferred to the payee cannot be spent until this second stage of online settlement has occurred**.**

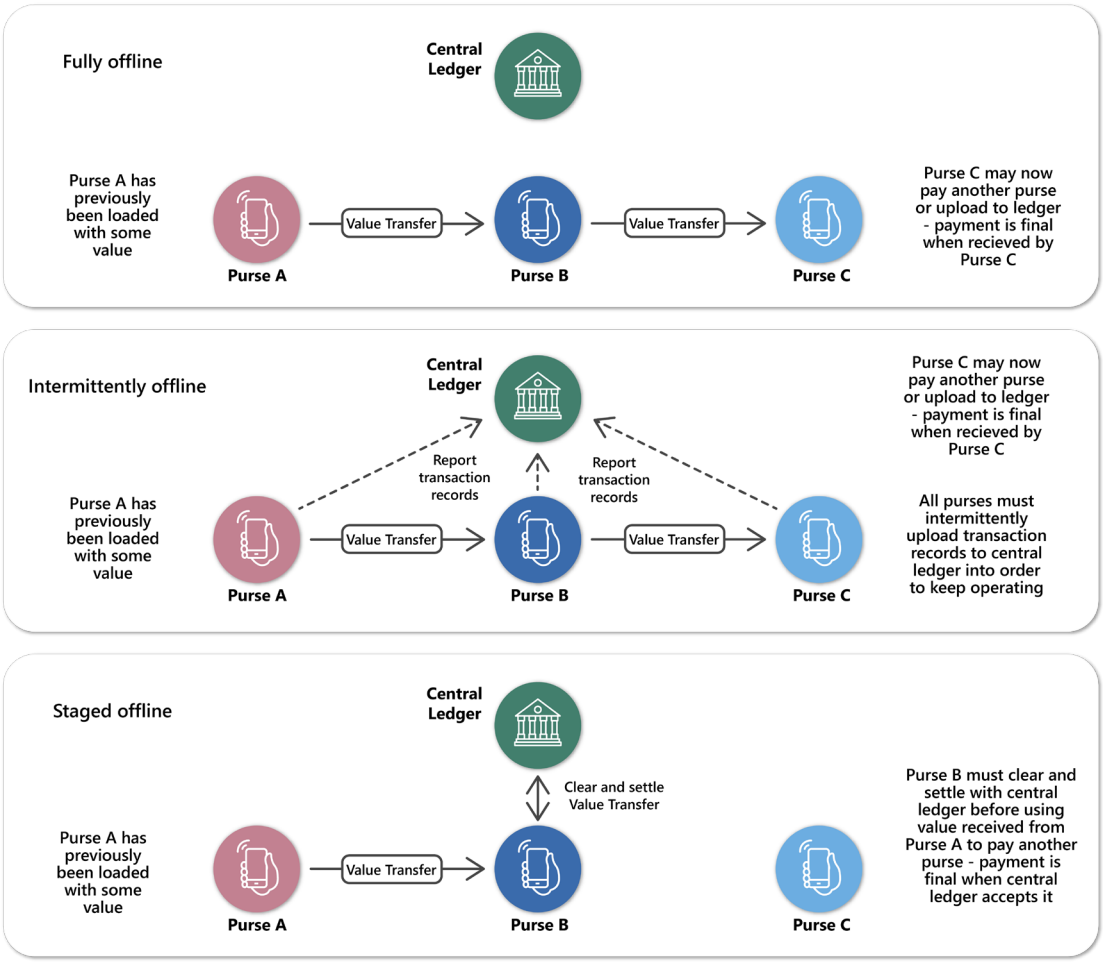
Figure 2 illustrates these different modes

[8] Some solutions could potentially support more than one mode for risk-management purposes. A solution could switch from one mode to another, for example when a certain limit has been reached a fully offline solution could switch to either intermittently or staged offline modes, before preventing further transactions.

[9] Settlement finality refers to when the transfer of funds is irrevocable and unconditional. Settlement finality is a legal concept, and this handbook does not use the term. Even though this is a desirable feature in offline payments, it may not be feasible in all arrangements since it would ultimately rely on the design of the system and the legal framework, for example bankruptcy law. Here "final settlement" is used instead to indicate that the transfer is final from a technical point of view, allowing value to be onward spent.

Modes of offline payment

Figure 2



Both fully and intermittently offline modes enable the payee to spend the value received at the end of the transfer. For illustration purposes, for both of these modes this figure shows only two transfers, the first between purses A and B and the second between purses B and C. In practice solutions would support more than two transfers, subject to any specific limits.

A brief history of offline payment systems

Offline payment systems existed before the prevalence of the internet or smartphones. While the infrastructure may have changed, many of the same issues remain relevant. A summary of various examples of payment systems from history, either specifically offline or otherwise relevant, are summarised below. Annex C provides a more detailed discussion of these systems.

Over the past three decades, there has been a range of offline payment solutions deployed:

- **Electronic purse systems (1990s):** For example, Digicash[10] (denominated digital coins), Mondex[11] (unaccounted offline value supporting automated lost value recovery) and Proton/Dancoin/Chipknip/Visa Cash (staged offline, accounted purses)[12] were all developed during the 1990s. Bank of Finland's Avant, claimed to be the world's first CBDC, was based on a smartcard solution (reloadable and non-reloadable).[13]

  These pioneering offline digital payment methods reflect the diversity of approaches to offline payments still in use today. Attempts to replicate physical cash too closely can lead to overly restrictive processes. Perhaps the most important lesson from these early systems is the need for a sound commercial model and the importance of user experience.

- **EMV Offline (1990s onwards):** EMV Offline, the ability to transact offline with payment cards, served an important purpose, enabling people to transact even without network connectivity. Indeed, pockets of EMV Offline still exist across the world. Its comprehensive processing capabilities demonstrate the measures which can be taken to achieve secure and resilient processing offline. These are comparable to today's staged offline solutions, which support offline transactions as a fallback for online payments but which require payees to go online to clear and settle value before it is available for further spending.

- **Offline contactless payments in mass transit (2000s onwards):** Starting with Transport for London (TfL) in 2012, mass transit systems around the world have used contactless EMV solutions which demonstrate the power of combining offline and online capabilities. Initial checks can be run quickly offline, with further processing taking place online. Rather than being a fallback, the offline capability is selected in the first instance because it can support rapid, scalable, high-volume processing.

---

10 An overview of Digicash is given in Abrar (2014).

11 Stalder and Clement (1999) provide a good description of Mondex.

12 The common European electronic purses of the 1990s are reviewed in European Money Institute (1996).

13 For more on Avant, see Grym (2020).

- **M-PESA (2000s onwards):** Although not strictly offline, M-PESA[14] demonstrates how mobile money can be very effective where limited bandwidth is available. It remains a highly successful payment system, having expanded to Tanzania, Mozambique, Democratic Republic of the Congo, Lesotho, Ghana and Egypt and spawned a wide range of similar systems. It clearly demonstrates the importance of inclusion and tailoring the service to the local context and the needs of the people who will use it, and therefore provides an important lesson on usability.

- **TAP (2000s):** TAP demonstrated the use of a mesh system to synchronise multiple offline devices with a central system. Its demise, despite a successful pilot, shows the need for a sustainable commercial model.

- **qSPARC (2016):** The Quick Specification for Payment Application of RuPay Chip (qSPARC) specification based on offline payments in transit systems in India works on the concept of immediate payment from an on-device purse on a RuPay card and deferred settlement through an intermittently online mechanism. It uses EMV concepts to enable the creation of both multiple on-device purses on the same card for offline payments for use with multiple closed loop transit operators or a single general purse for offline payments to interoperable transit operators.

[14] For background on M-PESA, see Hughes and Lonie (2007).

3.3 Key lessons from history relevant to offline payments with CBDC

These historical examples provide several lessons for the implementation of offline payments with CBDC:

- Security: tamper-resistant purses and cryptographic protocols allowing devices to mutually authenticate themselves and exchange payment instructions securely are enduring requirements.
- Risks: double-spending and counterfeiting of value are ongoing concerns. It is essential to detect situations where value is lost in transit and needs to be recovered or otherwise accounted for (or it be assumed that the value is lost forever).
- Operational processes: the master cryptographic keys that protect payment processes need to be kept secure. The availability of mobile computing devices now means that payment applications may be provisioned while in a user's hand. This presents new challenges that historical offline payment solutions did not face.
- User experience: at the time most of these solutions were deployed the ability to make the user experience better than the alternative of cash was limited. For example, contactless solutions had yet to be deployed and the smartphone had not been invented. In more recent years, the successful adoption of PIX, the smartphone based instant payment solution available in Brazil, highlights the importance of user experience in achieving adoption of new payment methods.
- Commercial model: many historical offline payment solutions struggled to offer a commercial model that solved the problem of attracting both payers (mainly individuals) and payees (mainly merchants) and generating enough value to make it worthwhile for intermediaries to support them. This could be an important consideration when introducing offline payments with CBDC.

Overall, the technical challenges and solutions remain similar.

4 Offline payment solutions with CBDC

4. Offline payment solutions for CBDC

There is a range of offline payment solutions available today from private-sector companies. All are at various stages of development, with each providing different components and therefore not all of the features and functions that could be required. Many of these solutions rely on a single type of user device to host an offline purse. The type of solution has implications for the design of a CBDC system.

A number of solution vendors were interviewed to develop a logical architecture,[15] and the common attributes and capabilities of these offline payment solutions, including their features and functions, are discussed in this section.

4.1 Logical architecture for offline payment solutions

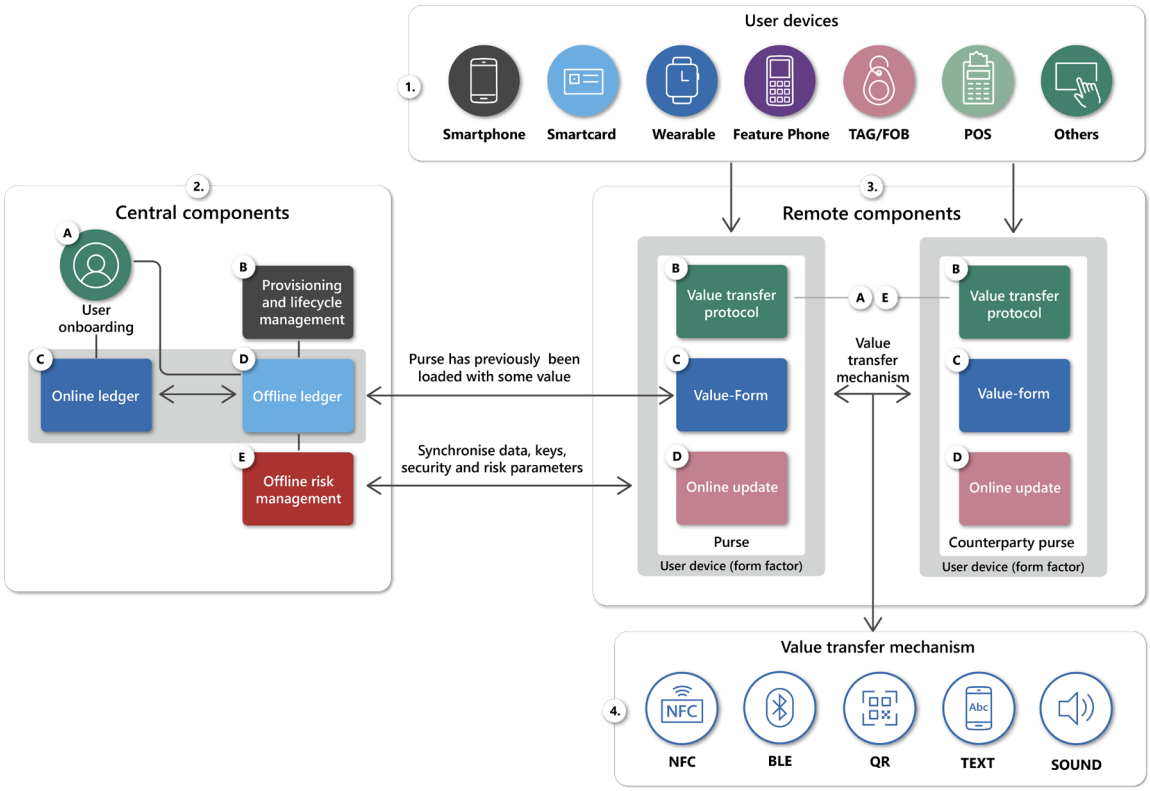
Figure 3 represents the key logical components required to support offline payments functionality in CBDC systems. This is a simplified view for the purposes of this section and should not be regarded as a design for a full operational solution.

Components may vary in actual implementation; for example, online and offline ledgers are represented as two distinct components in order to distinguish between the features and functions of each, but they could be provided as a single component.

Integration with other systems and funding or defunding paths are out of scope.

[15] The number of vendors interviewed was limited by time constraints and the availability of vendor representatives. The inclusion of any specific vendor should not be taken as an endorsement of their products, while the exclusion of any vendor does not indicate any issues with their solutions.

A logical architecture for offline CBDC payment solutions Figure 3



This logical architecture makes no assumptions about the type of technology the ledger may use nor how this is provided, with different solution vendors taking different approaches.

The components of the logical architecture are summarised below:

1) **Tamper-resistant user devices (also known as form factors)** describe the types of tamper-resistant user devices that could support offline payments with CBDC.

2) **Central components:**

   a) **User onboarding** covers the process of onboarding users into a CBDC system, including AML and KYC requirements.

   b) **Provisioning and life cycle management** covers how offline CBDC purses could be deployed and updated, including the issue of cryptographic key management.

   c) **Online ledger** covers the aspects of an online CBDC ledger required to support some offline CBDC capabilities.

   d) **Offline ledger** covers the possible approaches to delivering an offline CBDC ledger representing the value held in offline purses.

e) **Offline risk management** describes possible solutions for managing certain risks associated with offline payments. This could include the ability to define and update parameters such as limits or to receive transaction logs.

3) Remote components

a) **Purse** represents the software implementing the offline payment functionality installed on a user device, and includes:

b) **Value transfer protocol** covers the methods used to transmit payment instructions between one user device and another.

c) **Value-form** covers the representation of how value is stored in a purse.[16]

d) **Online update** considers the methods employed on user devices to provide the centralised systems with updates about the status of the offline CBDCs deployed on a user device.

e) **Counterparty purse** is a representation of another offline purse involved in an offline transaction. Both the purse and the counterparty purse are the same component discussed later on.

4) **Value transfer mechanism** refers to the technologies available for communicating between devices, for example near-field communication (NFC).

4.2 Tamper-resistant user devices

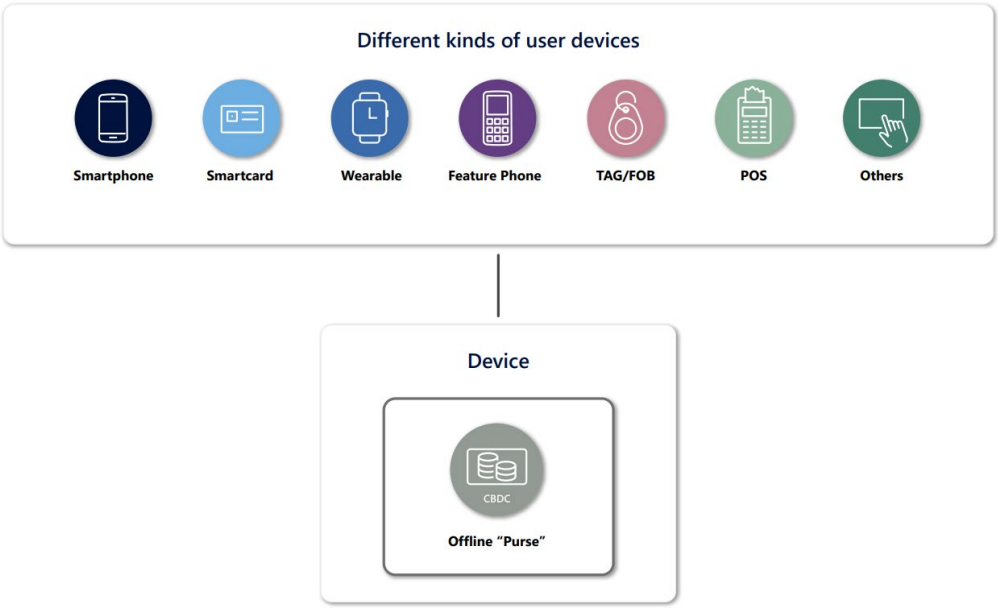
The ability of user devices to protect data stored in purses is critical for offline payment solutions. Any solution will depend on the tamper resistance of the user device to protect against physical and cyber attacks.

There are two types of approach, hardware-based and software-based, although combinations of both are common. Both hardware and software approaches offer several variations in how they implement tamper resistance.

In all cases, the user device and purse combination must be designed to be tamper-resistant, because they will need to hold cryptographic keys and other data, such as the value-form and risk parameters, securely and perform cryptographic operations using those keys and data. Access to and exposure of these keys or data could result in a security breach; it is therefore critical that the hardware or software make this as hard to achieve as possible.

[16] Offline payment solutions for CBDC are often referred to as either "account-based" or "token-based". For this handbook, this distinction has not been used as most solutions are either or both. System requirements will determine the suitability of a solution and the value-form used.

Types of tamper-resistant user device Figure 4



4.2.1 Secure element (SE)-based

Hardware based-solutions are based on tamper-resistant chips, for example those commonly used in EMV payment cards.[17] These chips are referred to as "secure elements". Some smartphones may contain a secure element, although not all do.

These secure elements are generally certified to high levels of security assurance and offer a range of tamper-resistant qualities, including resistance to physical attacks and side-channel attacks. Some SIM cards in mobile devices also meet these security standards.

Secure elements support secure provisioning methods which protect the loading of applications and data to the secure element. These methods are usually compliant with the GlobalPlatform[18] standards.

[17] See EMVCo (2022). For readers interested in the range of attacks that EMV certification is designed to prevent, we recommend reading "3.3.6 Assess product and product provider infrastructure". The list of attacks on secure elements is ever-evolving.

[18] See GlobalPlatform (2018a). GlobalPlatform is a technical standards organization that enables the launch and management of secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity and convenience to users. It provides standardized technologies and certifications, developed through effective industry-driven collaboration, that enable technology and service providers to develop, certify, deploy and manage digital services and devices in line with security, regulatory and data protection needs. GlobalPlatform technologies are used in billions of smart cards, smartphones, wearables and other connected and IoT devices to enable convenient and trusted digital services across different sectors. These standards would be relevant for many offline payment solutions.

Secure elements are relatively expensive and may not be available or suitable in all cases, particularly in countries where smartphones or EMV-based smartcards are not widely available.

4.2.2 Trusted execution environment (TEE)-based

Many smartphones contain a trusted execution environment (TEE), which is a means of enhancing the security of mobile devices. The TEE is a part of the smartphone hardware[19] that allows software applications installed on the device to securely execute code and to process and store data, all in isolation so they cannot be viewed or modified by other processes or software applications running on the device.[20] It is intended as a means of enhancing the security of mobile devices and allowing code to be executed and data to be stored and processed.

TEE-based mobile applications may require support from other applications or services implemented in the mobile device in order to provide tamper resistance. For example, protection against other attacks such as side-channel attacks or rooting (jailbreaking), both of which are discussed later on, depend on the smartphone's own processing capabilities and any countermeasures implemented in the rest of the device.

Although TEEs typically offer more functionality than SEs, they offer a lower level of tamper resistance than an SE and are certified to lower levels of security assurance. Mobile applications using TEEs will need to be separately tested and certified.

Like with SEs, TEEs support secure provisioning methods which protect the loading of applications and data to the secure element. These methods are also usually compliant with the relevant Global Platform[21] standards.

4.2.3 Secure software-based

Software-based solutions are typically smartphone-based and use a range of software techniques to protect cryptographic keys and data both at rest and while they are being processed. Unlike hardware-based solutions, they do not require specialised components to execute their applications.

Software solutions typically offer lower levels of tamper resistance than SEs or TEEs,[22] and could use commercially available "white-box solutions" to provide tamper resistance.[23] Software solutions would need to be separately evaluated, risk assessed and certified for assurance.

---

19 TEEs are also used in other devices and are not specific to smartphones.

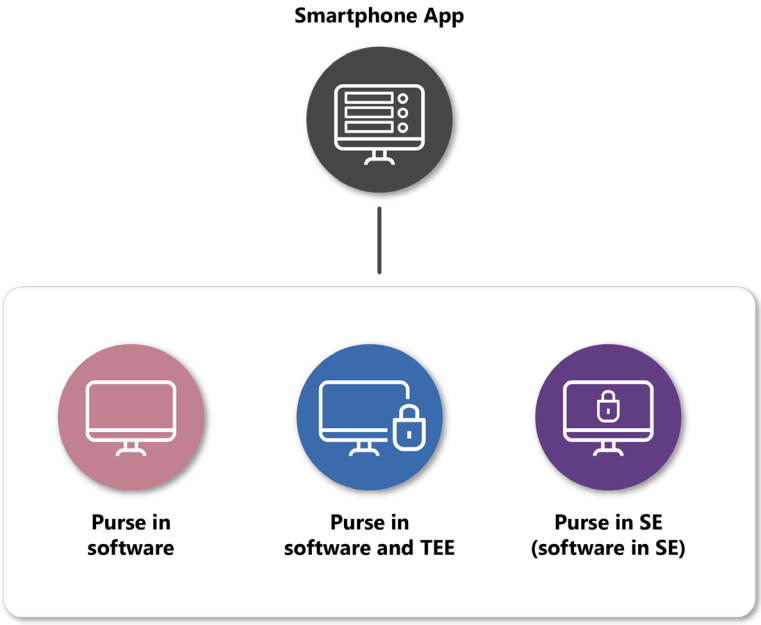
20 See Trusted Labs (2013).

21 See Global Platform (2018b).

22 Secure software-based solutions could also use TEEs or SEs where these are available to support the required protections.

23 For example, see Bock et al (2020). White-box cryptography is a complex area, with ever-evolving protection methods and potential attacks.

Deployment options for purses on smartphones Figure 5



4.3 User onboarding

User onboarding processes and the supporting system functionality will be required for any CBDC system and are not specific to an offline payments use case. However, user onboarding has specific implications for the type and level of privacy that an offline payment solution has and how this is implemented, so a system's user onboarding functions should take into consideration several factors:

- **The type of user** – for instance, merchant onboarding may be different from consumer onboarding.
- **The type of product being issued** – for instance, a user device only supporting low-value transactions, for example a fob, may require minimal or no identity checks.
- **The level of identity check carried out** could influence the limits applied. A basic identity check, for example based only on a mobile phone number, could allow only low-value transactions, but a full identity check could allow higher-value ones.
- **Compliance with existing rules and regulations** – for instance, Know-Your-Customer or Know-Your-Business (KYC/KYB), Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and data protection rules.
- **The level of privacy required in offline payments** – for example, whether some form of identity is required to be exchanged during an offline payment.

Whilst many solutions include privacy by design, users could be identified if their anonymous purse identifiers are linked to identity information provided during onboarding processes or to other unique identifiers, such as mobile phone numbers, which could be part of the value transfer protocol.

Consideration will need to be given as to which entities are permitted to perform user onboarding and what the authorisation scheme and the associated rules and regulations, including liabilities, may need to be. For example, if user onboarding allows a bad actor into the system, it may allow them to commit fraud. Offline payments where transactions cannot be monitored may be an opportunity for such fraudsters.

4.4 Provisioning and life cycle management

Each type of offline solution will require processes that cover the production, issuance and management of purses and user devices. These processes are expected to meet the highest level of security standards so that both the value and information stored is secure. The processes covered include secure provisioning, cryptographic key generation, reprovisioning and deprovisioning[24].

4.4.1 Secure provisioning processes

Hardware-based user devices need to be provisioned along with their purses, including confidential information such as the purse's cryptographic keys. This would require secure processes in secure facilities operating under strict rules on physical and information security. This ensures that data and cryptographic keys are kept secure, and is similar to processes used today to provision credit and debit cards.

For example, secure provisioning would be needed for smartcard-based solutions that require some association to an individual (even if an individual's identity is anonymised); a unique identifier on the purse may be used to achieve this.

Secure provisioning processes are required to produce SEs. They are typically controlled by the device manufacturer and certified by an independent party.

Secure software solutions, whether they leverage SEs or TEEs, have their own provisioning processes. Understanding the provisioning processes a solution vendor uses and how the level security of the software will remain robust over time (ie through a secure software development lifecycle) is important.

Purse security will depend upon the security of the purse provisioning processes and how a purse is subsequently updated.

[24] See GlobalPlatform (2018a)

4.4.2 Cryptographic key generation processes

Cryptographic key generation processes are critical as these keys ensure the security of the value transfer protocols and value-form.

Cryptographic keys can either be generated in a secure processing facility and provisioned into the purses or generated directly in the purses.

Key provisioning and generation processes should be analysed to ensure that they are appropriately secure. This is the case for both hardware- and software-based solutions, although hardware-based ones should be expected to use the existing secure provisioning and key generation mechanisms supported by the device.

4.4.3 Lifecycle management activities

Reprovisioning of a purse, because of a necessary refresh, new purchase, or loss or damage to a new or replacement user device, should consider how any existing offline value can be retrieved from an old purse and reloaded into a new purse.

Deprovisioning of user devices for example due to loss, security reasons or at the user's request, may involve simply blocking the ability to use a device beyond a certain point.

4.5 Online and offline ledgers

CBDC systems will have a ledger of some form, which is represented as an online and an offline ledger (which could in practice be a single component) in the logical architecture.

An online ledger is used by the online CBDC solution and will also provide some of the features and functionality required to successfully implement offline CBDC payments.

4.5.1 Fully offline solutions

Depending on the value-form, an offline ledger may not be required, though without it transaction monitoring will be a challenge. Any online ledger may be unaware of any offline payments, except for top-ups to and deposits from offline purses.

4.5.2 Staged offline and intermittently offline solutions

Staged offline and intermittently offline solutions require an offline ledger component to record and reconcile the value in an offline purse. An offline ledger provides a representation of the current known state of an offline purse. This may not be the real-time or actual state, as a purse can transact offline, but the ledger is updated at some point after transactions take place when devices go online.

For both solutions, there can be alternative implementations of the online ledger/offline ledger design:

- **Separate balances** - The online ledger supports separate online and offline balances (no separate offline ledger is required). The online ledger can support offline ledger capabilities such as synchronisation with offline purses.
- **Separate ledgers** -The offline payment solution supplies its own offline ledger.

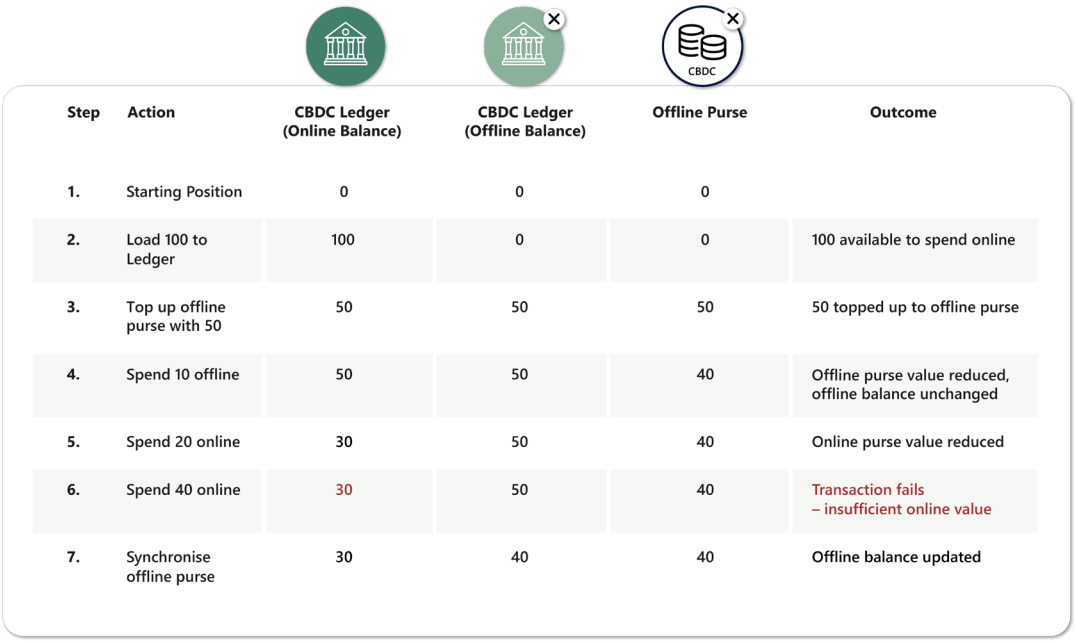
The offline ledger (or an offline balance associated with the online ledger) should identify the value held in the offline purse as distinct from the value held in the online ledger. It is important that any online balances and offline balances are segregated, otherwise it may be possible for a user to spend the same value both offline and online and create a double-spend risk[25]. This segregation applies to the underlying technical implementation.

The design of the user experience around the difference between offline and online balances is important, as users could get confused when they have sufficient overall CBDC value across both online and offline balances but are still unable to pay. It should be clear to users which balance they are using, though this could be dependent on the solution. Users should also have the choice to use their offline balance in an online situation.

Figure 6 illustrates an online transaction failing because there is insufficient online balance available, even though there is enough offline value to complete the payment.

[25] Segregation of online and offline balances does not eliminate the risk of double spending and other measures to mitigate this risk may be required.

Online vs offline balance segregation Figure 6



Step	Action	CBDC Ledger (Online Balance)	CBDC Ledger (Offline Balance)	Offline Purse	Outcome
1.	Starting Position	0	0	0	
2.	Load 100 to Ledger	100	0	0	100 available to spend online
3.	Top up offline purse with 50	50	50	50	50 topped up to offline purse
4.	Spend 10 offline	50	50	40	Offline purse value reduced, offline balance unchanged
5.	Spend 20 online	30	50	40	Online purse value reduced
6.	Spend 40 online	30	50	40	Transaction fails – insufficient online value
7.	Synchronise offline purse	30	40	40	Offline balance updated

4.6 Offline risk management

Risk management is a critical component of offline payment solutions. Most offline solutions include specific components for risk management, provided either separately or as integrated features. The maturity of these components varies, and further work is required to understand what central banks may need and what incident management would involve when certain issues are detected. Such components provide the following features:

4.6.1 Risk parameter management

A risk management component manages risk parameters, for example limits on balances, transaction value, velocity and volume. This can be enforced locally in the user device and purse, and could be updated, or pushed, from a central risk management system when an offline purse comes online to the ledger, in the case of intermittently or staged offline solutions, or when making a payment when in contact with a connected device such as a PoS terminal.

Fully offline purses may still support risk parameter updates, but this would only be possible when the purses come online to top up or deposit funds.

4.6.2 Transaction history management

Many solutions allow transaction history information to be retrieved from purses. This can be at the level of the transactions undertaken by a specific device or as a history of the chain of transactions.

In the latter case, each payment made contains a history of the chain of transactions since last online, which could allow ledger systems to recreate offline transaction histories. This could allow risk management systems to detect anomalies or potential financial crimes, albeit at an undetermined point after any suspicious transactions have taken place as monitoring cannot happen in real-time. However, such solutions require additional complexity in purse designs, greater communication bandwidth and potentially more frequent updates.

4.6.3 Limiting the lifetime or uses of cryptographic keys

Purses may limit the number of uses or the lifetime of specific cryptographic keys for risk management purposes. In software-based purses, it is common to require keys and associated certificates to be refreshed periodically, but devices may need to have access to sufficient network bandwidth in order to allow for new keys to be uploaded, which may not always be possible. This would create trade-offs between security and network accessibility.

4.6.4 Block list management

The risk management component may detect an issue, for example the presence of a compromised device that is capable of injecting counterfeit CBDC value into the system; risk management systems would need to provide mechanisms to block or isolate it. In practice, this may be difficult to achieve in a timely manner, particularly if a compromised device continues to operate without connecting online or to another connected device.

Incident management plans and readiness activities must take these types of incidents into account.

The ability to roll out block lists of compromised purses to stop genuine purses from transacting with them is one option for incident management. However, the design for this needs to reflect the memory requirements it imposes on purses and the length of time it may take to roll out. For example, this may be easier to roll out to and enforce on PoS devices versus a smartcard.

4.7 Purses

Purse application software should be run within a tamper-resistant user device. This will perform a range of functions, including some or all of the following:

- managing a secure value transfer protocol to allow secure offline payments to be made to other purses on other user devices;
- providing methods to mutually authenticate with other purses;;
- supporting the value transfer mechanisms, such as data processing and cryptographic algorithms, used to implement the value transfer protocol;
- managing purse balances, in whatever form they are presented;

- holding and/or generating the value-form used to transfer value between purses;

- managing interactions with online systems for risk management purposes;

- securely storing data, such as the value form or parameters for risk management or operations, as well as the cryptographic keys using the methods made available by the user device on which the purse is deployed; and

- supporting some form of user authentication to allow the user to prove their identity to the purse.

Not all purses may require or provide all of these features, but considering purse software against each of these points is an important part of evaluating a solution. Any poorly implemented purses could expose offline payment methods to a range of possible attacks.

The user device on which a purse is deployed could be used in different ways; for example, a purse could be deployed within a point-of-sale (PoS) device to allow for acceptance of offline payments with CBDC at merchants.

4.8 Value transfer protocol

Current solutions mainly use some form of public key cryptography, which allows user devices and/or purses to mutually authenticate each other (check that they are genuine), exchange keys and send signed messages which can be checked on the receiving device. Value transfer protocols can be:

- **two-way (bidirectional)**, where payer and payee devices need to communicate synchronously in real time to transfer value; or

- **one-way (unidirectional)**, where payer and payee devices communicate asynchronously, not in real time, to transfer value.

Many value transfer protocols assume bidirectional communication, which provides greater reliability around payment transaction completion.[26]

Unidirectional value transfer protocols mean a payer purse can generate a payment instruction, for example a code, in the absence of the payee purse and can supply it to the payee asynchronously, for example verbally. These could be useful where devices are not in constant communication, there is limited to no connectivity, or in

[26] They can also assume a shared time-based protocol between two devices. Where a solution leverages TEE and there is a shared time base, secure multi-party computation can be carried out between the two devices. Payment data should only be shared after a successful payment and to prevent attempts to exploit the value transfer protocol for information.

other specific scenarios. However, they could create challenges for the management of lost value .

The value transfer protocol determines whether:

- offline value transfers are final and available for onward offline spend (fully or intermittently offline), or

- offline value transfers may need to be cleared and settled online before they can be used for further offline payments (staged offline).

4.9 Value-form

The value-form is a representation of how an amount of value is stored in a purse. The way this is represented is variable; for example, it could be a cryptographically computed token or "coin". This could have an impact on other aspects of the CBDC system. For example, it could affect how and to what extent risk management systems are able to build a view of transaction histories.

Some examples of the value-form are:

- **A generic amount in a specific currency,** for example a transfer of €100 resulting in the decrease in a balance on the sending device and the increase in a balance on the receiving device.
- **A pre-determined amount (denomination) in a specific currency,** for example the transfer of a token or "coin" representing €100 and another representing €10, ie denomination in a specific value, similar to a physical currency.
- **The amount being transferred and the history of previous transactions,** which supports either fungible value transfers or denominated coin transfers. With this type of value-form, the transaction history can build up, meaning that the value-form can increase in data size and the user device reaches storage capacity; therefore, at some point this data must be offloaded and reconciled online in order to free up capacity and manage the size of the data transfer.

These differences between value-forms mean that many offline payment solutions may not be interoperable. This could be an important consideration when analysing requirements for providing offline payments functionality where more than one type of solution is made available or for future-proofing systems. Interoperability is discussed later on, but this is an area requiring further work.

4.10 Online updates

Offline solutions would need to connect online at some point to receive risk management or device updates[27]. These could include:

- risk parameter updates, for example limits, which alter specific thresholds in the purse and typically need to be operational as soon as received;
- cryptographic key updates;
- updates that block or restrict devices that are not up to date with the latest software or patches, or that are perhaps tampered with; and
- transmission of transaction histories.

Online updates can carry a burden in terms of network connectivity. For example, the size of messages either updating cryptographic keys or risk parameters or transmitting transaction histories will vary depending on the solution. The network bandwidth or communication protocol required to support these would depend on the design of the offline payment solution. This could pose a challenge in countries where bandwidth may be limited or unreliable.

4.11 Value transfer mechanism

Value transfer mechanisms are how the value-form is transferred between two purses and can be based on communication media or addressing mechanisms which include:

- **Near-field communication (NFC)**, also referred to as contactless, is a common approach to allowing devices to interact. Many acceptance devices, such as merchant PoS devices, support NFC as standard.

- **Bluetooth low energy (BLE)** can be very effective in specific situations, but there are potential issues in scenarios where there are requirements for high data bandwidth or there is a high volume of devices transmitting, making it difficult to pair with a counterparty device.

- **Text-based** solutions allow the value transfer message to be provided as text[28] by the payer, for example via SMS or other means, and typed into a payee device. These have the virtue of being almost universally supported, but could have limited usefulness depending on the scenario.

- **Audio signal-based** transfer mechanisms allow secure offline payments between relatively low-end devices, for example feature phones, using basic features such as the speaker and microphone. A user's device can generate an audio-based

[27] Fully offline solutions could continue transact without connecting online, however the user may need to receive essential device update for security or other reasons.

[28] Text could be a generated code from the payer's device. The payer would send this to the payee, who would enter it into their user device.

message or pulse signal sent to a receiver, which can transmit that message to another device via other means.

- **Quick response (QR) codes** are a common and simple addressing mechanism for initiating payments and are used by some offline payment solutions.

Each mechanism may have limitations, such as scalability, and some may be more useful in certain use cases than others, so it may be desirable to support a combination of mechanisms depending on the use case and requirements.

The type of protocol or value-form selected may determine which value transfer mechanisms can be supported. For example, a value-form that includes the history of all offline transactions since the device last connected to a ledger system may be too large to be effectively communicated over low-bandwidth value transfer mechanisms.

There are also other options that could be used as a means of exchange – for example, so-called hybrid banknotes, which have a face value but also have digital representation, such as a QR code (akin to the serial numbers found on notes today), which can be reconciled back to a ledger.[29] The note can act as an offline value transfer mechanism.

4.12 Interoperability

Interoperability is key to the user experience, utility, acceptance and adoption of CBDC. For CBDC systems to support offline payments, two main interoperability issues need to be considered: interoperability between different offline solutions, and interoperability between online and offline solutions.[30] [31]

4.12.1 Between different offline solutions

Many of the solutions for offline payments are not interoperable. Selecting a specific solution could impede the adoption of other solutions, which could have an impact on cash resemblance objectives. Lack of standards could be an obstacle to achieving interoperability.

Although more work is needed to analyse interoperability issues, it seems unlikely that this can be resolved at a purse level such that a purse from one vendor can make an offline payment to a purse from another vendor. Support for more than one solution will require careful consideration and coordination with the private sector.

---

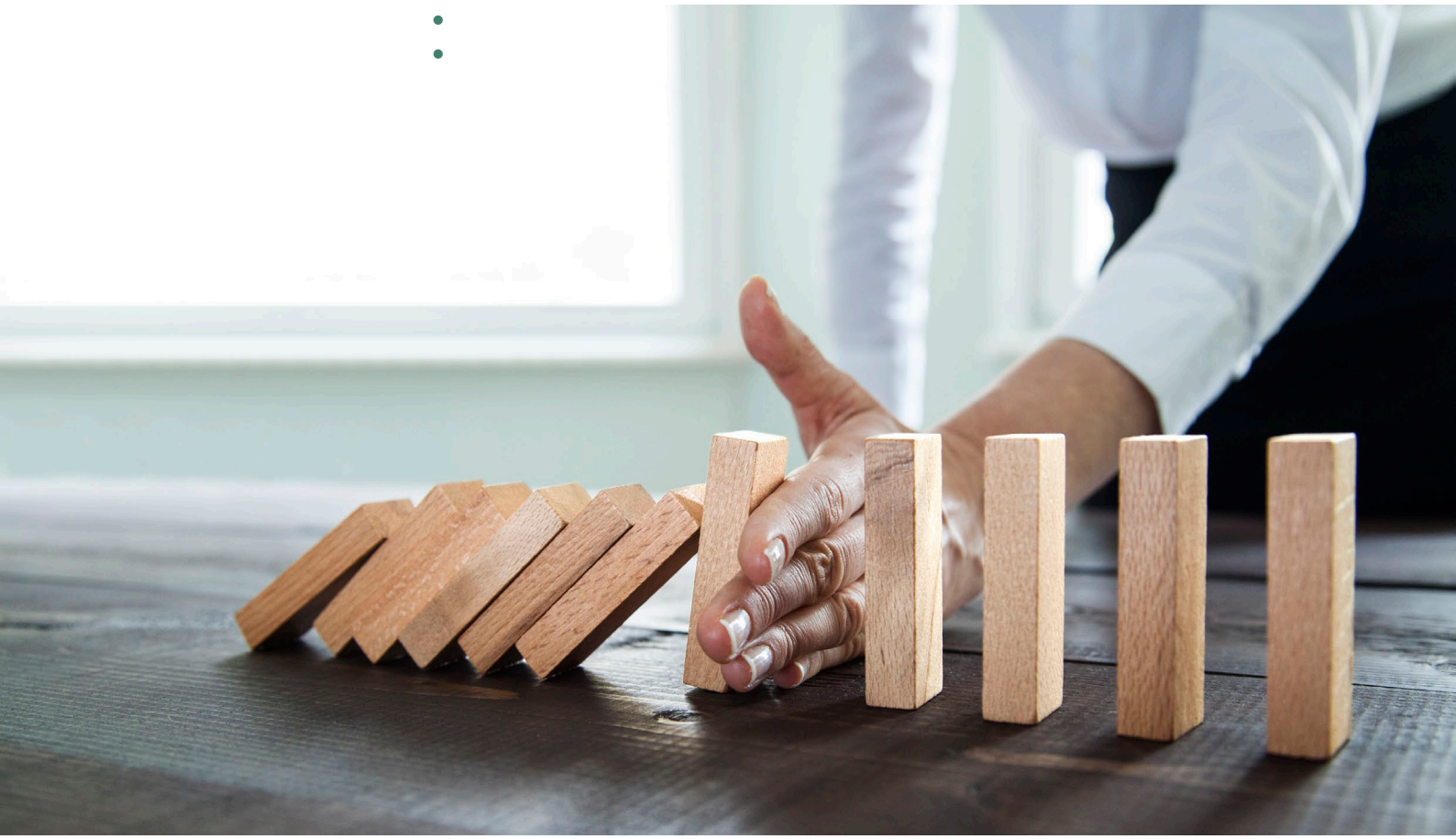
29 For example, see Noll and Lipkin (2021).

30 Further work may need to consider how offline payment solutions for CBDC could interoperate with traditional solutions, perhaps for usability and user experience reasons, but this is out of scope of this handbook.

31 Interoperability is also important to ensure there is choice between multiple solutions in order to cater to different needs as well as to avoid creating "walled gardens" or limiting users to a specific vendor.

4.12.2 Between online and offline solutions

In analysing solutions, central banks should consider the technical integration between online and offline payment systems, which would be a complex challenge. Consideration would need to be given to the user experience of how online and offline balances are made clear to users, as well as to how the combined solution would handle transfers between online and offline payments across a range of use cases.



5 Risk management by design

5. Risk management by design

In CBDC systems, risk management by design is key. This needs to be considered from the outset such that risk management measures are built into both technology and operational processes and the relevant organisational risk management capabilities are established across the actors in a CBDC ecosystem.

This is particularly important for CBDC systems that provide offline payments functionality, as offline payment solutions are exposed to different threats and vulnerabilities, and therefore different risks, than online solutions.

For example, with fully or intermittently offline payments, any transferred value would immediately be available for onward spend, so the risk of value creation arising from the threat of counterfeiting could be difficult to detect and block.

In this context:

- A risk refers to the potential for destruction, damage or loss of business assets and data resulting from a threat.
- A threat is an event that unintentionally or intentionally exploits a vulnerability to damage, destroy or obtain an asset.
- A vulnerability is a weakness in networks, hardware, software or processes which a threat actor exploits to damage, destroy or obtain an asset.

Risk is a function of threats and vulnerabilities with a probability of occurring, resulting in some form of impact.

Potential threats and vulnerabilities and the level of risk each poses are based on their impact on the confidentiality, integrity and availability of systems, data and networks as well as the overall business impact assessment. This chapter outlines the main threats and vulnerabilities faced by offline payment solutions, as well as the possible risk mitigation measures.

Determining whether a specific solution is sufficiently secure will require investigation into multiple factors, covering the user device as well as the purse application running on it, the risk management processes supported by the system components, and the operational processes that the central bank and the solution vendors will manage.

Most solution vendors design their solutions to make them as difficult as possible to breach and to ensure that the cost of an attack outweighs the value gained.

Risk types can be categorised as:

- **Technology risks** – the risk that any technology failure will disrupt an entity's business or operations.
- **Operational risks** – the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

- **Reputational risks** – the risk of reputational damage to an entity when it fails to meet the expectations of its stakeholders and this is negatively perceived.

Risks can belong to one or more of the categories above. Each would need to be carefully assessed and mitigated through either technical or non-technical risk management measures or a combination of both, with some element of residual risk that would have to be deemed acceptable to the organisation. There may be other kinds of risk in connection with offline payments, for example legal risks, that are out of scope of this handbook. The degree of risk each presents may vary by country, capabilities, infrastructure and solution used.

5.1 Key assumptions

The key assumptions in this section are:

- Any payment system will be attacked or face some form of technology failure. In particular, there is a wide range of possible attacks on offline payment solutions, including breaching physical devices, redirecting value-forms or replaying value-forms.
- As with cash, there will be attempts to counterfeit CBDC when held as offline value.
- Fraud is inherent in all payment systems, despite real-time (or near real-time) risk analysis.[32] Offline payments cannot benefit from real-time risk monitoring and analysis and must adopt alternative measures.
- No security measure is ever completely unbreakable – security is always an arms race – so CBDC systems must make provision for future changes to their risk management methods.

5.2 Threats and vulnerabilities

This section discusses the main possible threats and vulnerabilities a central bank or solution vendor may need to consider for offline payments with CBDC.[33]

5.2.1 Counterfeiting via physical breaches

With offline CBDC payments, some representation of CBDC value will be held in a purse on a user device such as a smartcard or in storage on a mobile phone.

---

[32] For example, the Cybersource *Global fraud and payments report* for 2022 identified that 3.6% of e-commerce revenue was lost to fraud in 2022.

[33] Denial of service is a threat to an overall CBDC system which could in turn have an impact on some aspects of offline functionality. This is not discussed in this handbook.

Threat actors[34] may seek to clone or manipulate this value-form and the means of transferring it through intrusive, physical attacks on the device, eg by attempting to read or alter data through micro-probing.[35] As the user device may be in the possession of the attacker, they could have unlimited time to mount such attacks without being detected.

5.2.2 Counterfeiting via cryptographic protocol analysis (cryptanalysis)

There are also non-intrusive approaches to counterfeiting. In an offline value transfer, there will be a point at which value is being transferred between purses. This transfer will be cryptographically protected. If the cryptographic keys used to protect these transfers can be recovered and reverse engineered, it could be possible to generate fake messages and counterfeit value. This type of attack tends to be less common today and well-designed value transfer protocols should protect against such attacks, however advances in cryptanalysis means this remains a threat and should be taken into consideration.

5.2.3 Side-channel attacks

A side-channel attack occurs when an attacker tries to access data inside a device by attacking it from the outside, by exploiting information leaked by the device.[36] For example, an attacker could:

- measure and perform signal analysis on the electromagnetic radiation emitted;
- monitor variations in the electrical power consumption or electromagnetic emissions of a target device;
- analyse the time spent executing different cryptographic algorithms; or
- recover cryptographic keys by exploiting an identical device and comparing data exploited via side channels.

These sophisticated attack vectors could allow an attacker with sufficient time, expertise and equipment to recreate cryptographic keys and therefore potentially create counterfeit value.[37]

5.2.4 Fault-inducing attacks

Another form of attack on a secure element is to induce faults during cryptographic processing by placing it under stress through some external method, eg heat or

---

[34] Threat actors refer to groups, individuals or entities that intentionally seek to cause harm. Some examples of threat actors relevant for offline payments could include nation states, organized crime groups, hacktivists or individuals seeking financial gain.

[35] For example, see Skorobogatov (2017).

[36] For example, see Matthews (2006).

[37] For example, a recent study carried out an AI-assisted attack, using recursive training and side-channel data, on a public key encryption algorithm recommended for post-quantum cryptography. See Dubrova et al (2022).

radiation. Cryptanalysts may then be able to deduce key values by comparing outputs.[38]

5.2.5 Cryptography strength, lifetime and ability to update

Crypto-durability is a measure of how long a cryptographic system or algorithm can remain secure against potential threats and attacks without requiring significant changes or updates. This is important for offline payment solutions because cryptographic keys and algorithms are used to protect stored value and sensitive information for various periods of time.

Crypto-agility refers to the ability of a cryptographic system or algorithm to be updated or replaced with a new, more secure algorithm or system, allowing the system to adapt to new threats and attacks by quickly and efficiently implementing new cryptographic methods. This is important for offline payment solutions, for example in the event of a breach.

Both cryptographic keys and cryptographic algorithms have a limited lifetime, as advances in processing power following Moore's Law[39] and in technology make it easier to break ever-longer keys and complex algorithms. Therefore, it is important for CBDC systems to be able to update cryptography (ie be crypto-agile) when required.

Both crypto-durability and crypto-agility are important for CBDC systems in order to maintain the confidentiality, integrity and availability of data and systems over time, in the face of evolving threats and increasing attacks on digital systems.

5.2.6 Master cryptographic key compromise

Offline value transfer protocols, including the value-form and any value transported by them, will be protected by cryptographic keys. If master keys or centralised key generation systems are exposed, it may compromise the entire system and could, for example, allow payment instructions and/or purses to be counterfeited. The physical security measures, robust controls and operational management required to protect these keys are therefore critical in ensuring the ongoing security of solutions.

5.2.7 Third-party device compromise

Offline payments may need to use third-party devices, such as smartphones or feature phones, over which central banks and vendors may have limited control.

Third-party devices may be compromised due to security weaknesses that are detected and exploited by threat actors or by users accidentally or deliberately compromising the security of their devices, for example by rooting or jailbreaking smartphones, which could affect the security of the device. Note that these problems are experienced by both offline and online payment solutions (eg where the online

---

38 For example, see Biham and Shamir (1997).

39 Moore's Law is the empirical observation that computing power roughly doubles every two years.

payment solution is using an app on a smartphone to transact), but the challenges for offline payments will usually be greater as some form of value will be exposed on the device.

Software-based purses, for example on smartphones, could be exposed to malware attacks on mobile devices and will need to be designed to limit the amount of information they leak during processing. Where third-party devices use secure elements or TEEs, they will be more resistant to device compromise, as these components are securely segregated from the rest of the device. Nonetheless, compromised devices may be exploited by malware to attempt fraudulent transactions.

5.3 Risks

5.3.1 Device obsolescence

Older devices may become obsolete when they are no longer supported by the solution provider or when relevant security or other updates cannot be provided. In some cases, attempted and successful attacks on obsolete devices may cause reputational risk as they could undermine trust in offline payment solutions.

5.3.2 Double-spending

Double-spending is related to a number of the previous threats and refers to situations where the same offline value is spent a number of times and, without the possibility of performing an online check, the recipient cannot be sure that the funds they have received are still in possession of the payer.

It is important to note that the double-spend issue for offline CBDC payments is different from the well-publicised double-spend issues for public cryptocurrencies. In the former, trust rests in the tamper-resistant nature of the user device and the purse's shared cryptographic protocols, while in the latter trust is based on consensus mechanisms, essentially a form of clearing message. A well-designed offline value transfer protocol should ensure that double-spend attempts will be rejected by the payee's purse.

5.3.3 Fraud

Criminals will attempt to exploit payment methods in order to divert funds or goods to themselves.

In particular, instant payment systems, where the payment value is instantly settled on the payee, have been fertile ground for fraudsters, mainly by persuading users, through social engineering attacks, to send them money which they can then immediately disburse to other accounts.[40]

[40] There is a good description of the various types of authorised push payment fraud in UK Finance (2021).

Fraudsters may also attempt to persuade users to pay them by impersonating parties known to the user – either personally or as businesses. The ability to identify payees may be necessary to prevent this type of fraud, although this can conflict with requirements for privacy and solutions that support privacy by design.

Central banks should consider these types of fraud, which cannot be blocked by payment systems, in the context of the overall design of their CBDC solutions, including liability protections and user experience design where appropriate.

5.3.4 Lost value

One consequence of offline payments is that offline value can get lost. At a high level, four different scenarios can be considered:

- **A user device is lost** – the offline value on a device is no longer available to the user but could, in theory, be spent by someone who gains possession of the device.
- **The user device is broken** – the offline value on it is no longer available to the user or any other party.
- **A transaction is torn** – value has left the payer purse and has not been received by the payee purse.
- **Value is forgotten** – a user leaves CBDC value on their user device and forgets about it.

The first two scenarios may interact with the third, eg a lost or broken user device may have been involved in a torn transaction such that offline value may be missing and not available to any purse.

Lost user device

If a user loses their device, the value on it is still valid and therefore could be spent by someone else who gains access to the device.

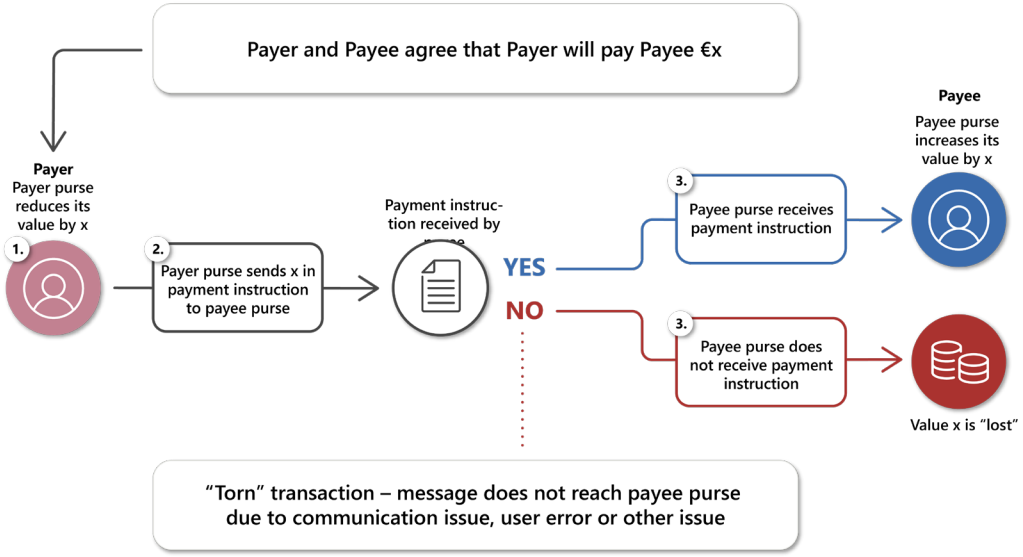
Broken user device

In any population-scale system, cases where a user device is broken and unable to transact can occur, leaving value locked on that device which cannot be spent. The situation is similar to the lost device scenario, with the exception that the user should be able to provide proof that their device is broken and unusable.

Torn transaction

In any offline payment transaction, there is a point at which the value has been removed from the payer purse but has not been updated on the payee purse. This is true regardless of the value-form used and the commit procedure used to instruct the purses to change their states. Figure 7 below illustrates this:

An illustration of a torn transaction Figure 7



This time delay means that there is some possibility that the transaction will be interrupted just at the point where the payer purse has acted on the payment instruction but before it has been acted on by the payee purse.

This is known as a "torn" transaction and it means the value has been lost in transit. Some technical mechanisms exist to recover torn transactions, but there will be occasions where this is not possible and value recovery becomes an issue of policy for a central bank.

However, torn transactions may also occur because a notification from the payee purse indicating it has received and acted on the payment instruction has not been received by the payer purse. In this case, the value transfer completed successfully but the payer purse would not know whether the instruction was received and acted on or was not received at all.

Forgotten value

Value held offline on a user device may get lost because a user has forgotten about it. For example, users may obtain a new device and forget to transfer the value, or they stop using or are unable to use the device and any value is forgotten.

5.3.5 Third-party vendors and supply chains

Third-party vendor systems may contain faults or otherwise not work as expected due to errors in code, mistakes in configurations and problems caused by system upgrades. Additionally, third-party systems will use components and services from other vendors, which themselves may result in threats to the supply chain.

Third-party systems can also be intentionally compromised by threat actors to introduce software weakness, as in the SolarWinds attack.[41]

These issues are not unique to offline payments, but they will need to be addressed for all CBDC payment solutions procured wholly or partially from third-parties.

5.3.6 Lack of risk management and breach detection

Although offline payment systems rely on the tamper resistance of user devices and the cryptographic security of value transfer protocols, this must be supported by risk management both in purses and in online systems. For example, purses need to be updated with risk parameters which they can apply to payment transactions in order to restrict what rogue counterparty purses can do.

In addition, online CBDC systems need to carry out risk analysis and breach detection. This is also true for offline payments, including fully offline solutions, where some potential issues could be identified by monitoring value flows through online points of connection for top-ups and deposits.

Being unable to analyse offline payments to detect potential breaches, and therefore unable to respond to such an incident, could expose central banks to reputational, operational and legal risks.

5.3.7 Complexity of the technology stack

CBDC systems may introduce technologies that may not be well understood, tested or previously implemented in a central bank. This could increase reliance on third-party expertise rather than on internal staff, where it may take time to establish training, skills and capabilities. This could introduce operational risks.

5.3.8 Insider threats

Internal staff roles with privileged access, such as IT administrators or system operators, accidentally or deliberately affect system operations or create financial gain. This applies to both online and offline systems.

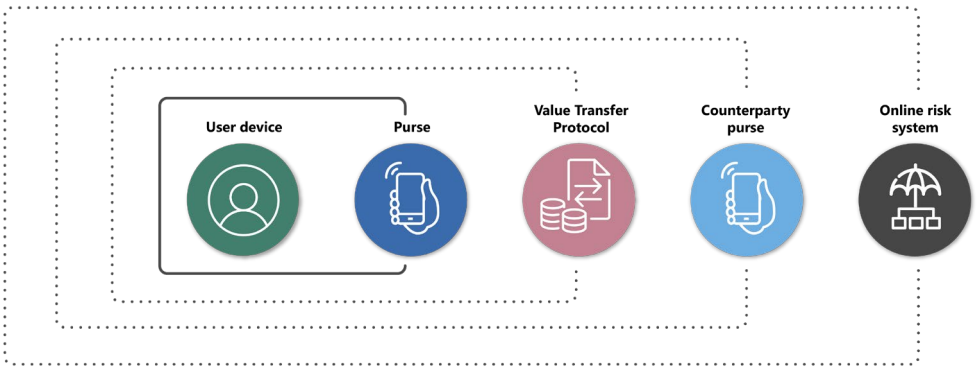
5.4 Risk management measures

The threats and vulnerabilities in the previous section can apply across one or more of the risk types. Therefore, a range of both technical and non-technical risk management measures would need to be implemented. This section outlines a number of risk management measures that could be applied to the threats and vulnerabilities listed above based on the risk assessment. This is not exhaustive and concentrates on a few key measures.

---

[41] A malicious actor discovered a way to compromise a software update service for one of the SolarWinds products. The actor was able to compromise the update channel used by the product to distribute malware.

A simplified view of the layers of risk management components Figure 8



The above figure shows a simplified model of the risk management components that must be applied to offline payment systems:

- **User devices:** User devices must be capable of securely storing and processing data and cryptographic keys for some defined and extended period of time.
- **Purse:** The purse software must secure stored data, including the value-form and cryptographic keys.
- **Value transfer protocol:** This protocol must ensure that the value-form cannot be tampered with or replayed (for example double-spent). Cryptographic processes are used to implement these protocols.
- **Counterparty purse:** The counterparty purse involved in an offline payment is an important component of offline security. A counterparty purse could implement risk rules to limit the amount of value that can be exchanged with a rogue device or even block transactions involving that device.
- **Online risk systems:** Risk systems are needed to monitor the state of the system, including the amount of value flowing through it, in order to collect transaction records (except for fully offline systems), clear transactions (for staged or intermittently offline systems), update risk parameters and, in some cases, refresh cryptographic keys on offline devices.

5.5 Technology risk management

There are no perfect technologies, so any CBDC system design must reflect this. Certain criteria should be enshrined within the design of the solution to ensure that system breaches can be managed.

5.5.1 General criteria

	Criteria	Description
1	Limits on the scope of an attack	Any successful attack on the system should have limited effect. For example, if CBDC value is loaded into a purse on a secure element and that purse is breached, then the breach should not affect other purses on other secure elements.
2	Limits on the scalability of an attack	Any successful attack on the system should not be scalable. For example, successfully attacking a single device carrying CBDC value should not make it easier to attack other devices.
3	Limits on the economic cost of an attack	Ideally, the cost of any single attack on the system should be more expensive than the value that could be obtained from it. Note, however, that even where economic attacks are unfeasible there will be people and organisations that mount attacks to inflict reputational damage and loss of confidence or for their own reputational gain. This covers not just the defence of any specific purse on a user device, but also the ability of an attacker to cash out. For example, there should be limits on how much value can be transferred out of a purse to another purse or to an online account.
4	Methods to detect that a breach has taken place	With offline payments, it may be hard to detect that a breach has occurred. Systems must be designed to ensure that such breaches can be detected. Even so, detection will happen after the breach has occurred, as the payment will occur offline before online systems are updated.
5	Methods to react to a detected breach	Systems should support methods to isolate compromised purses, for example by downloading block lists of compromised purses to other purses or

		tightening offline risk checks to manage breaches.
6	Methods to ensure that the system's security can be upgraded	Advances in technology and decreasing costs will allow for future attacks that are not possible at the time of development. Systems must be capable of being upgraded to defend against these future threats.

5.5.2 Measures to mitigate the risk of counterfeiting

In general

- It should be difficult to "cash out" of the system; even if it is possible to create large amounts of counterfeit value, an attacker should only be able to pay out small amounts at a time, mitigating their ability to inject large amounts of counterfeit money into the system, which is also limited by risk controls elsewhere, for example on counterparty purses or online systems.

Via device breach

- The degree of tamper resistance offered by a user device (provided by secure elements, trusted execution environments (TEE) or secure software) and the cryptographic security protecting the value in purses and user devices are important.
- User devices with a high degree of tamper resistance may be used for any type of solution, but would be a key requirement for fully offline solutions.
- User devices with lower degrees of tamper resistance would be unsuitable for fully offline solutions, but could be used for intermittently offline solutions, along with an appropriate synchronisation regime, as well as for staged offline solutions, where payees would need to accept liability if transactions are not settled before goods or services are supplied.
- The data elements representing value, offline risk parameters and associated cryptographic keys must be stored securely and encrypted in situ to prevent them from being cloned and used.
- Protection of the cryptographic keys involved in the offline payments process requires careful design of the key hierarchy and domains so that a breach of an individual device does not imply an automatic breach of all other similar user devices. This could increase the costs of mounting an attack, as each additional device would also need to be breached.

Via cryptographic protocol analysis

- The cryptographic algorithms used to protect the value-form during value transfers should be reviewed and certified by appropriately qualified experts.

- Algorithms should protect against
    - replay attacks (repeating the transfer of the same value-form);
    - modification (changing the value-form); and
    - redirecting (sending a genuine value-form to a different purse from that originally intended).
- Value-forms may need to be transmitted confidentially to prevent eavesdropping.

5.5.3 Measures to mitigate side-channel attacks

- Effective side-channel measures should be implemented at the design stage. Hardware-based user devices should be certified against such attacks, and software-based purses should be specifically tested against these measures.
- A properly certified SE should have built-in defences that mitigate the chances of a successful side-channel attack either by reducing the leakage of side-channel information or by masking it with fake operations to produce information indistinguishable from that generated through normal operations.
- TEEs provide support for side-channel attack defences.
- Software-based purses will need to be designed to limit the amount of information they leak during purse processing. They will need to be specifically tested to ensure they are robust against known attacks for the period during which their cryptographic keys are valid.
- Software-based purses may need to have their keys refreshed on a regular basis, depending on the solution, in order to limit the effectiveness of such attacks.

5.5.4 Measures to mitigate crypto-durability and crypto-agility risks

- Offline payment solutions must include mechanisms to allow both cryptographic keys and algorithms to be changed when required or upgraded over time.
- Certain frameworks can be used to assess the risk posed by a lack of crypto-agility.[42]
- CBDC systems, whether online or offline, must be crypto-agile enabled by technology deployment and operational processes designed to support this easily and effectively.
- Cryptographic keys with limited lifetimes or uses could be applied, dependent on the value-form used, and refreshed periodically.

5.5.5 Measures to mitigate risks of master cryptographic key compromise

- Facilities managing master cryptographic keys and key generation processes should have bank vault-equivalent security, with high levels of physical security and security protocols in place to manage those keys.

[42] Ma et al (2021) introduce a framework for assessing crypto-agility.

- These facilities should use appropriately certified tamper-resistant hardware security modules (HSMs) to store and protect cryptographic keys.
- Some secure hardware-based user devices may use the purse's software in conjunction with the device's own cryptographic capabilities to generate the master keys, ensuring that private keys remain private to the purses. However, this may not always be possible for operational and logistical reasons.
- Where purses require their cryptographic keys and risk parameters to be periodically updated, these should be refreshed more frequently than an attacker would be able to breach the purse software and user device hardware.
- Where keys are pushed to or retrieved from an external repository, for example a cloud-based service, robust controls should be put in place.

5.5.6 Measures to mitigate risks from third-party device compromise

- Any device hosting a purse should still be supported by its manufacturer with security updates. These updates should be applied, reversing rooting or jailbreaking if possible.
- If a device is unsupported, has not been updated, or is rooted or jailbroken, a purse should not be able to be hosted or able to operate.
- The purse software should be able to detect such issues and suspend offline payments in such cases. However, these issues could be difficult to detect, so security should not rely solely on this.
- The purse software will need to be specifically tested to ensure it is robust against known attacks for the period during which its cryptographic keys are valid. For example, software-based purses may need to have their keys refreshed on a regular basis in order to limit the effectiveness of any attacks.
- Other safeguards to protect against potential attacks could include restrictions on the number of offline transactions that can be carried out before connecting to a ledger system.

5.5.7 Measures to mitigate risks from obsolescence

- Offline payment solutions should check the status of user devices. If the device is unsupported or not maintained with the latest security updates if should prevent payments from being initiated until the device is updated.
- However, any such checks are likely to be imperfect, as the mechanisms for detecting device status are not well defined and could be exploited by threat actors.
- Devices that are obsolete or suspended may have offline value loaded onto them. Depending on the design of the purse, it should be possible to restore and transfer this value back to an online account, assuming the device has not been compromised.

5.5.8 Measures to mitigate double-spending risks

- Any specific payment instruction should be accepted only once and by only one receiving purse. Repetition of the exact same payment instruction and attempts to spend the same value twice should be rejected by the receiving purse. Redirection of a payment instruction intended for one purse to another purse should also be rejected by the receiving purse.
- The methods for ensuring these requirements are met are well established, and are dependent on the physical security of cryptographic keys and data on tamper-resistant devices and cryptographic principles.
- Segregation of online and offline balances in the underlying technical implementation could also prevent spending the same value both online and offline.
- Intermittently and staged offline solutions could be a mitigating measure as they would need to connect online regularly.

5.5.9 Measures to mitigate fraud risks

- User authentication and transaction security methods equivalent to those for existing payment solutions in the local jurisdiction should be adopted. This is particularly important for offline payments, where online risk and fraud checks are not possible.
- It should not be possible for a user that is not the owner of the user device and purse to transact with it. In practice, however, the more onerous user authentication is, the less likely users are to engage with it.
- In order to mitigate against impersonation, where the payee pretends to be a different user, such as a merchant, it may be necessary to include mechanisms that allow payees to be identified. However, this may require analysis of the relevant use cases and consideration of any privacy issues.

Measures to mitigate lost value risks

Lost user device

If user devices are lost with value loaded onto them, the following issues should be considered:

- The lost purse can be blocked. However, as it can transact offline, the value may be spent before the purse block takes effect.
- Counterparty purses may be updated with block lists containing the missing purse. However, as they can transact offline, the value may be spent before these are received.
- If the lost purse is in the hands of a criminal, they will drain the value if they are able to access it.

A combination of policy and technology approaches could be required to determine how to manage cases of lost user devices. These could include:

- User authentication could limit potential losses, as users are typically required to keep their authentication details secret. If their device is lost or stolen and someone else finds it, then it should not be able to be used to make a payment.
- Payment service providers may take a risk-based view; for example, users who report their stolen device and lost value could be seen as trusted and their value restored, unless this happens on multiple occasions.
- If the lost purse has not transacted for a specific period and no other purse has been detected transacting with it, then value could be deemed lost and potentially restored automatically.[43]
- Purses could be designed to include time-limited value such that if the value is not spent offline within a certain period, the value will be automatically restored online. Automatic recovery mechanisms would require a structure in the value-form that allows expiry dates to be assigned, but this could create user experience issues, for example when the transfer of value is prevented as the value-form has expired. However, such automatic recovery mechanisms have not been used in a real-world setting and require further research and testing in order to better understand how they work in practice, how certain issues like double-spending are prevented, how online synchronisation would work, and what the limitations are, for example in an area with limited connectivity. This type of measure could be perceived as a restriction on the use of money and therefore could be undesirable in some cases.

- Not all offline payment solutions can store records of offline transactions. It could therefore be necessary to infer missing transactions from incomplete records. Some fully offline solutions may not keep any transaction records, so refund schemes will depend on policy. Lost purses could have been involved in torn transactions and could have the data necessary to establish the correct state. For example, the lost purse may have not received the value in a transaction which left the payer's purse but never arrived at the payee. In this case, online transaction records could indicate that the value was received by the purse, even though this may not have occurred. However, this can only be addressed by policy.
- Limits on how much value should be held offline are key to managing some lost value risks.
- The relevant policies for lost purses and refunds would need to be developed. The capabilities of the offline payment solution(s) could influence how this is done.

Broken user device

Policies and technical processes may need to be developed to:

[43] For example, see Kahn et al (2021).

- Recreate offline value on a broken device, notwithstanding issues with missing or torn transactions, and restore value to the online account, depending on policy.

- Block a broken device, where possible. In the event this broken device is somehow restored and the value on it accessible, this could prevent it from being spent, particularly if that value was already restored to an online account..

- In fully offline systems, purse value on broken devices is likely to be lost permanently.

Torn transactions

Offline payment solutions should include provision for handling torn transactions:

- The value transfer should resume and be completed if the connection between purses can be immediately restored.
- Users should be informed[44] and offered support on how to recover the transaction, where possible.
- If a transaction is torn and not recovered, then the purse should retain any data to help identify this. Different value transfer protocols may handle this in different ways, but:
  - A purse should retain records of transactions that are incomplete.
  - Transaction records should be recoverable by risk management systems.
  - If a risk management system can recover records from both purses involved in the torn transaction, it could restore the transaction to the correct state.
- Lost or stolen devices may contain records of torn transactions which will never be available to a ledger system. Policies for handling potential permanent value loss due to torn transactions may need to be developed.

Forgotten value

- The forgotten value could be treated as lost in the same way that cash left in a drawer or value left on an unused prepaid card would be.
- Some of the measures that apply to a lost device could also mitigate this risk.

5.5.10 Measures to mitigate third-party vendor and supply chain risks

- There should be a single function responsible for vendor management.

[44] The way of informing users of a torn transaction may vary depending on the solution and user device. For example, software-based solutions may be able to inform users via the mobile application they are using.

- Thorough due diligence should be carried out and central banks should be aware of the vendor's full supply chain, components used, certifications and assurance, and changes to the supply chain. This should be risk assessed on a regular basis.

- Vendors should also have robust security controls and certifications as specified by the central bank. The vendor should conform to the agreed-upon international security standards, for example ISO and NIST, or industry best practice. These controls and certifications should be regularly audited.

- Clear acceptance testing processes and security assurance should be in place to ensure that offline payment solutions are fully tested before they are released into production, including any future updates.

- Vendors and their third parties must immediately notify the central bank of any incidents.

- The facilities, systems and processes used to perform secure provisioning should be analysed and independently evaluated and assured.
- Clear understanding of how provisioning requests are initiated and linked to end users and how cryptographic keys are securely generated and provisioned to the end device is a critical part of security management for the program. This should also be independently evaluated and assured.

5.5.11 Measures to mitigate lack of real-time transaction monitoring and breach detection

Offline limits and checks

Offline payment solutions will need to be able to support checks, such as limits, as part of a set of countermeasures to reduce the impact of certain risks, for example counterfeiting or third-party device breaches. These checks would be executed during an offline payment by the purse software loaded onto the user device.

These checks could include elements such as:

- the maximum offline value that any purse may hold;
- the maximum offline payment that any purse may make;
- the maximum number of times that a purse may transact offline before going online;
- the maximum cumulative amount of value that a purse may transact offline before going online;
- the maximum value that a purse may transact offline without authenticating itself; and
- a list of counterparty purses that should not be transacted with.

Risk management requirements and the capabilities of the purse and the user device will affect the types of offline checks and limits that can be applied.

It should be possible to update offline checks and limits (risk parameters), which can happen when a purse connects to the central system. Further work may be required to understand the optimal approaches to and performance trade-offs with managing and updating limits.

Online risk management systems

Online risk management systems may need to analyse transaction data and gross flows of value from offline purses to detect anomalous behaviour. Offline payment solutions vary in how this is supported. Some solutions allow for the reconstruction of all historical offline payments back to a ledger, others support a partial reconstruction, and fully offline systems provide no offline transaction data. Fully offline solutions may need to interact with some online system periodically, for example to top up and deposit value, which could allow risk management systems to see flows of value or detect potential breaches.

Online risk management systems need to be able to react to breaches when detected. Possible responses include:

- preventing suspect purses from synchronising with online systems, including topping up and depositing value;
- updating risk parameters on purses to reflect changes in overall system status, eg restricting the size of offline payments; and
- updating risk parameters on purses to prevent them from transacting with suspected rogue purses.

Incident management and response

As part of the risk management for any payment system, how incidents are managed is crucial, particularly for offline payments.

In the worst case, a breach could lead to offline value being "created" outside of the central bank's process for issuing CBDC, which would require a coordinated response.

Based on this worst case scenario, central banks should design, prepare and be able to execute an incident response process that includes aspects such as:

- training the incident response team;
- ensuring there are clear roles and responsibilities and there is an accountable executive for incident management and that the incident response team are supported by senior leadership;
- categorising the types of incidents and establishing how they are identified and whose responsibility it is to do this;
- ensuring there is a clear set of responsibilities and processes in place for escalating and responding to incidents once they are identified;
- identifying what countermeasures are available to deal with incidents once they are detected – for example, this would determine what risk parameter updates

might be needed and what their impact would be on the performance of the system, including potential performance issues if more purses were forced online more regularly;

- identifying whether subsets of purses or cryptographic keys need to be updated and, if they do, ensuring that this process is managed and, where needed, communicated effectively to users;
- developing a communications plan for dealing with incidents – in some cases there may be regulatory requirements to disclose breaches while in others it may be necessary to communicate with users to explain why their purses need to be replaced, and this may include responding to media queries where third parties have published claims about the security of the offline CBDC system;
- ensuring that all internal and external parties affected by the incident are promptly informed of incidents and their roles and responsibilities in the response; and
- including requirements for a solution vendor regarding incident response and recovery in contracts.

It is important that an incident management process be put in place before any offline CBDC payment solution is launched, as this may have an impact on the functionality and design of the solution. For example, effective incident management requires processes to support technical solutions for monitoring, detecting and addressing potential breaches.

5.6 Operational risk management

Operating a payment system comes with significant risks. If components from multiple vendors are being used, for example if the online and offline payment solutions have been developed separately then both would require integration. It may also be necessary to integrate ledger systems with risk management or other components. It is important that central banks establish who is responsible for these types of customisation activities as they can introduce implementation and operational risks:

- Clear service level agreements (SLAs) will need to be agreed with vendors providing operational systems, with clear contractual obligations and penalties to ensure that recovery time objectives (RTO) are met.
- Failures due to software issues need to be identified and addressed through service escalation plans with vendors, including root cause analysis and rapid and robust resolution of any issue.
- Central banks should ensure that there is complete transparency around and clear lines of responsibility for the third-party components used in order to prevent vendors from disputing any issues caused by their solution..
- Systems should be stress-tested to ensure that they are resilient to various failure conditions such as entire operational sites being taken offline and cyber attacks.

- Offline payment systems should provide risk monitoring and management services to detect and respond to attacks.

- Systems should be designed and tested to meet the central bank's performance and availability requirements. Any design and testing should take into account the chain of vendor dependencies, especially if solutions depend on third-party systems such as cloud-based hosting services.

- The possibility that vendors will stop support for critical national systems should be addressed in contractual obligations with the vendor. Central banks should have a default right to assume ownership over the solution, at no cost, if the solution vendor withdraws support. The latest version of the solution must be provided and stored with an escrow service approved by the central bank in the event that the vendor is unable to fulfil its obligations.

5.7 Reputational risk management

Some threat actors are motivated by potential financial gains, whilst others, such as nation-states, may be less interested in financial gain and instead place higher value on damaging the reputation of a country's central bank and wider economy.

The types of defence discussed in this section may not provide sufficient mitigation against reputational risk, especially if the threat actor mounting an attack is able to access the resources and equipment needed to mount such attacks without any cost restrictions.

Some other industries consider a range of non-technical approaches to mitigating reputational risk, for example providing bounties to individuals and organisations that privately detect and report issues on the understanding that these could be fixed before information is made public,[45] though such an approach would be unconventional for central banks.

The need to monitor offline payment systems becomes even more important in the context of reputational risk. If an offline CBDC system is under attack, it is important to be able to quickly detect this and react.

However, some threat actors may attempt to attack obsolete devices and old encryption methods or claim to have done so in order to create the perception that devices can be breached, which could undermine confidence and trust in the CBDC system and central bank

[45] For example, Google paid out $12 million through its Vulnerability Reward Program in 2022.

6 Privacy by design

6. Privacy by design

In the context of offline payments with CBDC, privacy issues typically focus on the balance between the need to support privacy (sometimes compared with that provided by cash or an individual's experience of using cash) and the need to combat money laundering, tax evasion and terrorist financing. The appropriate level(s) of privacy should be considered at the outset when designing a CBDC system, supported by the relevant policies.[46] This section considers the generally agreed privacy principles and how these could be applied to offline payments with CBDC.[47]

6.1 Privacy principles

The main, commonly agreed privacy principles are:

Privacy by design	Privacy should be incorporated at the earliest design stage.
Privacy by default	The default system settings should be the most privacy-enhancing.
Purpose for collection	The purpose should be declared at the point of data collection, with a clear description of storage and disposal.
Data minimisation and purpose limitation	A minimum amount of data should be retained for a limited time and used only for the agreed purpose.
Data protection	Data should be secured during collection, storage, use and disposal. Data should only be accessed at specific times and for specific purposes.
Data storage and anonymisation	Data should be stored securely. Data should be anonymised wherever possible. Regular audits should be performed.
User consent	Explicit user consent should be obtained when collecting personal data. Data may be disclosed to a third party only where necessary for service delivery. In exceptional circumstances, disclosure may be a legal requirement.
Individuals' rights	Individuals should have the right to access their own data or have them corrected or deleted within a reasonable timeframe.

[46] Offline payments may provide more private means of payment, but they are not the sole way to achieve this for CBDC systems.

[47] Subject to the relevant legislation in a jurisdiction and system requirements.

6.2 Privacy considerations for offline payments with CBDC

Offline payments with CBDC raise several privacy issues. These issues include the following:

	Issue	Consideration
1	**The types of solutions and limits that could be supported with minimal to no KYC/KYB checks on the user**	It may be possible to issue anonymous purses to users subject to specific risk controls and tolerance. For instance, anonymous purses may only be able to hold small balances or transact up to a certain amount. This may be important for inclusivity reasons. However, transactions from such purses may never appear on a ledger.
2	**The trade-off between privacy objectives and compliance with AML/CFT and KYC/KYB requirements**	Compliance with AML and KYC requirements could mean that transactions are ultimately traceable. Even if privacy is protected, transactions above a certain level may require identification of the payer. Transactions may need to be disclosed under legal mandate. Depending on the offline solution used, not all offline transactions can be recorded by a ledger. In cases where small transactions are permitted without identification or full KYC checks, offline payment solutions could be abused for money laundering techniques such as "smurfing", where large transactions are broken up into many small transactions to avoid detection.
3	**The level of privacy protection offered by the value transfer protocol**	If the offline value transfer protocol does not support privacy by design, then offline payments can never be anonymous.
4	**Identification and verification of counterparty users during offline payment transactions**	In some use cases it may be important for either the payee or the payer to identify the counterparty. For example, the payer may want to be assured of the identity of the payee (eg a merchant) , the details given to them are valid and their payment goes to the right place.. These transactions may not always involve face-to-face contact between the

		counterparties.[48] Impersonation fraud is a potential area of risk that central banks need to consider with regard to privacy.
5	**The difference between transaction anonymity and user anonymity**	For example, any authority with access to the ledger may be able to identify the users and the transactions they have executed, but counterparties may be anonymous to each other during a transaction.
6	**User identity attributes revealed**	Some personal data could be linked to a transaction, even if obfuscated. For example, if a purse is loaded onto a smartphone and the phone number is used to identify the purse, it may be possible to identify the user outside of the CBDC system.
7	**Legal or regulatory requirements to reveal a user's identity**	Legislation or regulations may require the ability to reveal users' identities even if the system protects these from all parties involved in managing the systems. For example, where it is suspected that offline CBDC payments are involved in proceeds of crime or money laundering activities.

There is no one-size-fits-all answer to the privacy questions associated with offline payments and CBDC systems generally, but these are critical and will vary by jurisdiction. Whatever choices are made, privacy by default should be the starting position as privacy is extremely hard to implement retroactively. It is easier to lower the level of privacy than it is to increase it. The highest level should be the starting point, with the option to lower the level of privacy as required (based on consent or on value-add services).

[48] Offline payments can occur remotely, where the only restriction is that the payments do not interact with the ledger. A user could potentially make an offline payment via the internet or a mobile network. Additionally, there are situations in which a payee may wish to reject a payment from a payer they cannot identify, eg a Bluetooth payment taking place in a crowded environment. Payments from unidentified users may sometimes be attempts to use third parties for money laundering purposes.

7 Inclusion by design

7. Inclusion by design

Inclusion by design caters to the needs of the whole population and aims to achieve widespread reach and acceptance. Any inclusion objectives should be considered from the outset of the design of CBDC systems.

These three aspects of inclusion should be considered:

- **Digital inclusion** – providing tools and skills to engage with digital systems
- **Financial inclusion** – enabling people to exercise financial self-determination and access financial services
- **Social inclusion** – enabling people to play an active role in society

7.1 Inclusion considerations

Some important considerations are outlined below:

Consideration	Issue	Inclusion aspects
User experience	Individual user capabilities, experiences and expectations will vary. For example, users with certain disabilities may have specific needs that may need to be provided for by different solutions. Designing inclusive offline payment user experiences will be critical to ensuring that everyone can use CBDC and that it gains widespread acceptance. Conventions are important. A payment solution may work for certain groups or regions but not work for others. This has an impact on adoption. It is also important to consider reasons why an individual or business may choose not to use or accept CBDC payments, even if they have the necessary skills and equipment.	Social, Financial, Digital
Whole population	All of society should be able to access and use CBDC.[49]	Social

[49] Consideration may need to be given to the methods that refugees, asylum seekers or migrants could use.

	Trust is paramount, and one aspect that ensures this is the implementation of privacy by design principles by working with local agencies and communities to understand any cultural and demographic factors and conventions that could affect system design choices. Apart from the social good of a payment system serving the whole population, there are also real commercial benefits to be derived from delivering at population scale. This can be valuable to individuals, local communities and the prosperity of a country as a whole. Particularly in areas where existing payment services are less well developed, appropriate payments mechanisms can support people's natural desire to expand the market for the goods and services that they offer.	
Accessibility	Not all users will have the same abilities, so offline payments must be designed to be inclusive regardless of background or digital competence. Any solution must be convenient and usable for the youngest and the eldest in society, as well as people with specific physical and mental impairments. This may require a variety of technologies, since no single technology can include everyone. For example, there are people who are unable to provide fingerprints and some who cannot reliably remember PINs. Touchscreens are not well suited to people with tremors and partially sighted people often need adapted devices to access digital services. There are many high-quality standards describing options to support people with disabilities. In every country, some proportion of the population has some kind of mental or physical challenge. Any public good should be designed to take their needs into account, guaranteeing provision to the whole of society.	Social, Digital

	These requirements must be identified at the outset since accessibility is hard to retrofit at a later stage.	
Financial exclusion	Offline payment solutions should not create exclusion and should be available to individuals or communities that typically prefer to use cash. Such solutions should also be available to those without bank accounts, reliable internet access, or access to mobile phones. In some cases, individuals may only have access to a feature phone or SIM card (for example, in some communities, some people may have their own SIM but may rely on someone else's phone).	Financial
Vulnerable individuals	CBDC may need to serve the most vulnerable in society. Design considerations may need to address people who are not legally resident in the country, people of no fixed abode or victims of harassment, who may not want their whereabouts disclosed. In some cases, the young and the elderly can be vulnerable to fraud, so processes may need to be designed to reduce this risk.	Social
Appropriate hardware	If offline payments are to be ubiquitous and support acceptance, they cannot depend on a single type of user device, particularly high-end smartphones. The ubiquity of smartphones is often overestimated. Even in prosperous societies such as the United States, smartphone penetration remains around 85%.[50] In other parts of the world, penetration rates are much lower. The huge success of mobile money such as M-PESA, based on feature phones using USSD (a basic mobile telephony service, sometimes referred to as "quick	Social, Digital

[50] Statista.com currently estimates US smartphone penetration at 85%+ of the population.

	codes"), demonstrates the value of tailoring the service to the local context. Offline payments will normally involve some kind of hardware: a smartphone, feature phone, standard smartcard, enhanced smartcard or bespoke devices such as wearables. In many cases, a combination of these may be adopted, eg a smartphone may operate as a POS device, while other user devices are used for peer-to-peer payments and to initiate payments at the POS.	
Infrastructure	Even in developed countries, not all people or locations have continuous access to core infrastructures such as internet, telecoms or electricity. Beyond the cost, functionality and availability of physical devices, it is important to plan around the availability of essential services such as network connectivity and electricity.	Social, Digital, Financial

A well-designed offline CBDC system must work in challenging circumstances while maintaining a convenient user experience. Apart from the above considerations, many design choices will depend on inclusivity requirements, the type of service to be provided, in what circumstances and for whom.[51]

7.2 Supporting multiple ways to pay

For CBDC to be accessible to everyone in society, more than one type of user device will be required. For example, purely smartphone-based solutions will not be accessible to all potential users who may instead use cards or feature phones. In the survey, some central banks mentioned that simpler technologies could be used for offline payments, therefore supporting inclusion objectives.

Although some vendors are looking to provide offline CBDC on multiple user devices, most are focused on a single type of user device. Each type of user device and solution has limitations which affect its suitability in different use cases.

[51] Services can be expanded in phases to meet inclusion objectives.

8 Resilience by design

8. Resilience by design

In the event of a system failure, cyber-attack or other adverse event, or in situations where internet or telecommunications connectivity is unavailable or unreliable, resilience measures can help ensure the public's access to basic payment services. Whatever choice the central bank makes on the level of resilience will be important for the design of the offline payment components of a CBDC system and should be considered at the outset of the design process.

Broadly, three themes emerged in the survey carried out in relation to this handbook:

- **short-term** resilience in the event that existing online payment solutions failed on a temporary basis;
- **ongoing** resilience to address areas where existing payment solutions were unable to provide services; and
- **civil contingency** resilience in the event of some catastrophic event causing the breakdown of the infrastructure supporting existing online payment solutions on an intermittent or semi-permanent basis.

Although similar, these three scenarios have quite different implications for the design of CBDC systems and how offline payments functionality would be provided.

8.1 Short-term resilience

This scenario occurs when there is some form of temporary outage with existing online payment systems and addresses the concerns from some central banks about the decline of physical cash as a backup for electronic payment systems. There is a wide range of potential temporary outage conditions, for example:

- an existing payment system or a mobile network suffers a temporary outage;
- a specific merchant is temporarily unable to accept some forms of electronic payment;
- temporary power cuts; and
- some types of cyber attack.

In these cases, offline payments would allow users to continue to transact.

8.2 Ongoing resilience

In some countries, there are geographic areas that are unserved by online electronic payment methods. This may be for a variety of reasons, such as the cost of providing these services or a lack of payments or mobile network infrastructure.

This resilience scenario is related to some of the inclusion themes mentioned above. In this scenario, offline payments with CBDC inherit some features of cash and coins,

allowing people to pay whenever and wherever. In the survey, some central banks mentioned that offline functionality provided by CBDC systems should be able to operate independently from existing infrastructure such as power grids and internet connections; however, further work may be required to better understand how this could work in practice, as well as the options and associated costs.

This scenario could be considered a permanent need, with offline payments with CBDC providing a public service supporting electronic payments for both merchant purchases and person-to-person transfers.

8.3 Civil contingency resilience

This resilience scenario relates to crisis situations. For example, in the survey, natural disasters, extreme weather conditions or war were commonly cited scenarios. In these situations, persistent access to online payment services may be severely disrupted or lost due to damage to infrastructure such as power, telecommunications or payment networks.

Such a scenario could extend over several months or longer. Offline payments could allow users to continue to transact despite damage to the infrastructure supporting online payment services, thought this has some limitations. In this scenario, the ability to perform P2P transfers is considered important by central banks.

8.4 Resilience considerations

Resilience by design has several considerations:

- **Lack of available offline CBDC value.** Where offline CBDC is intended to act as a stand-in for other payment services on a temporary or semi-permanent basis, there needs to be planning to ensure there is sufficient offline value available for the population's needs. By analogy, consider a similar situation where cash is expected to act as the fallback payment method. If no one has any cash when the situation occurs and ATMs are either scarce, not loaded or not working, then there is an immediate problem. A similar issue would occur with offline CBDC unless this contingency was planned for.
- **Commonality of acceptance infrastructure.** In some countries, the merchant acceptance infrastructure – primarily PoS devices – will be integrated to support all payment types. If these devices are no longer working, then they will not be able to accept any payment type, including offline CBDC. To avoid this, merchants would need a parallel acceptance solution for offline CBDC – cheap mobile phones, for instance.
- **Commonality of payment service providers.** One possible outage scenario involves the failure of specific payment service providers. In some jurisdictions, the intermediaries supporting CBDC payment services for users will also be payment service providers supporting other payment methods. A failure of such an intermediary would knock out all of the payment methods they support. Where offline CBDC payments require temporary connectivity to intermediaries to

refresh data and upload keys, this may lead to a failure of offline CBDC payments alongside other payment methods.

- **Offline CBDC payments do not support onward spending.** Some offline payment solutions, such as those that operate in a staged mode, do not support onward spending of a payment made until the payee goes online to clear and settle their funds before they are able to use them. This mode of offline payment may not be suitable for certain resilience scenarios and use case combinations. However, depending on the resilience scenario, allowing onward spending without online settlement could be acceptable for merchant payments if there is a scheme in place that provides merchants with certainty that offline payments with CBDC will be honoured (subject to the appropriate rules).
- **Risk rules limit offline payments availability.** In normal conditions, central banks and intermediaries may wish to limit the number or value of transactions that users can make offline in order to manage offline risk. However, in conditions where online systems cannot be reached, these risk rules may cause offline payments to stop working for a relatively short period of time.
- **Hidden dependencies**. If intermediaries or ledger operators are using shared technology such as cloud service providers and they suffer outages, then users may find themselves unable to transact offline due to an inability to synchronise to online systems. This is further amplified when multiple intermediaries use the same third parties.

8.5 Design considerations to improve resilience

Any implementation of offline payments with CBDC will need to be designed according to the type(s) of resilience required. Some considerations include:

- how users would be able to download offline CBDC value in the resilience scenarios described above and what the limitations are;
- whether alternative distribution models for CBDC exist or are required in advance of any issues occurring – for example, ATMs could be used as repositories, much like with banknotes;
- interoperability requirements, the type of value-form used and the costs of infrastructure;
- how operational processes supporting synchronisation of risk parameters, data and keys in these resilience scenarios would need to work;
- how necessary and timely updates, for example risk parameters, can be delivered in these resilience scenarios, ie what distributed risk management infrastructure would be required in order to provide multiple ways to connect to online services or for updates to be pushed virally;
- how risk parameters such as certain limits that may be common during normal circumstances may need to be relaxed in certain resilience scenarios and how policies like a government-backed guarantee may also need to be developed to allow payments to be accepted outside allowed risk parameters; and

- the possibility of providing reserve backup power sources for PoS terminals or increasing their capacity, and how the end-to-end aspects of the offline payment system can support improved resilience.
    - For example, PoS devices typically only support offline payments for a few hours, so some countries have taken measures to increase the capacity of PoS devices, thereby improving resilience in parts of their retail payment system.[52]
    - In some countries, some mobile phone manufacturers provide the ability to make payments when the device has run out of power[53]..

If offline payments with CBDC are seen as a permanent part of resilient measures for a digital payment ecosystem, combinations of the above points may be considered necessary.

[52] See Central Bank of Norway (2022).

[53] Some mobile manufacturers in China such as Xiaomi, Vivo and Oppo can already support e-CNY payment when the phone has lost power.

9 Conclusion

9. Conclusion

Offline payments with CBDC will be a complex part of the implementation of CBDC systems, and this handbook provides a comprehensive practical guide for central banks to inform their design and implementation plans whilst most central banks are in the early part of their journey.

There is no "one size fits all". The reasons for offline payments and envisaged use cases will vary by country. They should be supported by clear objectives for inclusion, privacy, resilience and how risks will be managed. These will influence both policy and technology decisions.

The CBDC ecosystem

The roles and responsibilities of the ecosystem in supporting offline payments need to be better defined, and collaboration between public and private sectors will be required.

Central banks should provide guidance to solution vendors on their expectations for what solutions should be able to offer.

Conversely, in some cases central banks may need to work within the limitations of a solution. No solution is likely to be an exact fit, and some compromise or trade-offs may need to be made. Solution vendors may not be able to run customised processes for each central bank, particularly with hardware-based solutions.

Security, risk and incident management

Security and operational requirements should be taken into account during the earliest stage of design, though any implementation should be kept as flexible as possible to accommodate any progress at the technical level.

The design of the overall solution must take this into consideration and ensure that the appropriate incident management processes are developed and the organisation is prepared.

Incident management, for example in the event of a device breach and value being fabricated, will likely be complex from both an operational and a reputational risk management point of view.

Some risks associated with offline payment solutions could be mitigated by a requirement to connect to ledger systems more frequently (such as intermittently or staged offline solutions), but this may involve a trade-off with supporting certain resilience scenarios or privacy objectives.

Policy and processes

Schemes including policies and processes may need to be developed to support situations where offline value is lost and cannot be recovered or users are defrauded. This could include dispute resolution processes.

Central banks should identify the appropriate balance between privacy objectives and AML/CFT requirements. This balance should be incorporated into the design of both policy and the technology from the outset, as privacy is hard to implement retroactively.

Policies and processes should be developed for risk parameters and how they are applied in both normal and certain resilience scenarios.

Further work

Interoperability and risk management systems for offline payments, for example the ability of solutions to detect and respond to potential breaches of offline purses and how different solutions can transfer value to each other, are two key areas that require further development.

Understanding how different types of solutions can fulfil privacy objectives as well as compliance requirements for AML/CFT, and what the trade-off could be between them, would benefit from further work.

Practical security-focused experiments addressing one or more of the threats listed in this handbook would also be beneficial.

Practical experiment focused on testing risk management measures such as the application of limits and also block-lists. For the latter, it would be useful to understand the risks (eg AML/CFT) of not being able to receive or apply a block-list in a timely manner.

Understanding who should bear risk and in what scenario, would be key.

General

Whilst this handbook discusses offline payments for a CBDC use case, it could also be useful for today's digital payment systems, where some offline payments could be useful for resilience reasons.

Offline payments can only provide an effective resilience layer if the right roles and responsibilities, processes, and infrastructure are in place and available.

This handbook may be updated in the future in line with developments with CBDC, offline payments, cyber security and technology.

10 References

10. References

Abrar, W (2014): "Untraceable electronic cash with Digicash", *Network and Communication Privacy,* 4 July.

Bank for International Settlements (BIS), Bank of Canada, Bank of England, Board of Governors of the Federal Reserve System, European Central Bank, Bank of Japan, Sveriges Riksbank and Swiss National Bank (2020): *Central bank digital currencies: foundational principles and core features*, 9 October.

Biham, E and A Shamir (1997): "Differential fault analysis of secret key cryptosystems", in *Advances in Cryptology – CRYPTO '97*, proceedings of the 17th Annual International Cryptology Conference, 17–21 August, pp 513–25.

Bock, E, A Amadori, C Brzuska and W Michiels (2020): "On the security goals of white-box cryptography", *IACR Transactions of Cryptographic Hardware and Embedded Systems*, vol 2020, no 2, 2 March, pp 327–57.

Central Bank of Norway (2022): *Finansiell infrastruktur*.

Cybersource (2022): *Global fraud and payments report 2022*.

Dubrova, E, K Ngo and J Gärtner (2022): "Breaking a fifth-order masked implementation of CRYSTALS-Kyber by copy-paste", *Cryptology ePrint Archive*, no 1713.

EMVCo (2022): *EMV® security guidelines, EMVCo security evaluation process*, version 5.3, December.

European Central Bank (2020): "Access to cash", ERPB/2020/031, 12 November.

European Money Institute (1996): *Payment systems in the European Union*, April.

Gao, Y, S Al-Sarawi and D Abbott (2020): "Physical unclonable functions", *Nature Electronics*, vol 3, no 2, pp 81–91, 24 February.

Global Platform (2018a): *Introduction to secure elements,* May.

——— (2018b): *Introduction to trusted execution environments,* May.

Glowka, M, A Kosse and R Szemere (2023): "Digital payments make gains but cash remains", *CPMI Briefs*, no 1, BIS Committee on Payments and Market Infrastructures (BIS CPMI), 31 January.

Grym, A (2020): "Lessons learned from the world's first CBDC", *BoF Economics Review*, no 8, Bank of Finland.

Hughes, N and S Lonie (2007): "M-PESA: mobile money for the "unbanked" turning cellphones into 24-hour tellers in Kenya", *Innovations: Technology, Governance, Globalization,* vol 2, no 1/2, April, pp 63–81.

Kahn, C, M van Oordt and Y Zhu (2021): "Best before? Expiring central bank digital currency and loss recovery", *Bank of Canada Staff Working Paper*, no 2021-67.

Ma, C, L Colon, J Dera, B Rashidi and V Garg (2021): "CARAF: Crypto Agility Risk Assessment Framework", *Journal of Cybersecurity*, vol 7, no 1.

Matthews, A (2006): "Low cost attacks on smart cards: the electromagnetic sidechannel", *Next Generation Security Software*, pp 1–15.

Mikkelsen, D, S Rajdev and V Stergiou (2022): *Managing financial crime risk in digital payments*, McKinsey & Company, 24 June.

Noll, F and A Lipkin (2021): "Smart banknotes and cryptobanknotes: hybrid banknotes for central bank digital currencies and cryptocurrency payments", *SSRN*, no 3974900.

Skorobogatov, S (2017): "How microprobing can attack encrypted memory", in *2017 Euromicro Conference on Digital System Design (DSD)*, IEEE, 30 August–1 September, pp 244–51.

Smart Card Alliance Payments Council (2014): "Technologies for payment fraud prevention: EMV, encryption and tokenization", white paper, no PC-14022, October.

Stalder, F and A Clement (1999): "Exploring policy issues of electronic cash: the Mondex case", *Canadian Journal of Communication,* vol 24, no 2, February.

Sveriges Riksbank (2022): "Offline payments can improve resilience to disruption", *Payments Report 2022*, 15 December.

Trusted Labs (2013): "Security evaluation of trusted execution environments: why and how?", white paper.

UK Finance (2021): *Fraud – the facts 2021: the definitive overview of payment industry fraud*, 25 March.

Wenninger, J and D Laster (1995): "The electronic purse", Federal Reserve Bank of New York, *Current Issues in Economics and Finance,* vol 1, no 1, April.

11 Acknowledgments

11. Acknowledgements

Bank for International Settlements

Beju Shah (Head of Nordic Centre, BIS Innovation Hub)

Susanne Bohman (Adviser)

Grímur Sigurðarson (Adviser)

William Zhang (Adviser)

Björn Segendorff (Adviser)

Hachem Hassan (Adviser)

Caroline Leung (Adviser)

Xin Zhang (Adviser)

Sidney Lampart (Adviser)

Consult Hyperion

Tim Richards, Principal Consultant

Margaret Ford, Head of Data Analytics and Insights

Neil McEvoy, Founder

Tim Allen, Sales Director EMEA

Harry Pounds, Consultant

Central banks & international organisations

Cyrus Minwalla, Fintech Technical Researcher (Bank of Canada)

Dinesh Shah, Director Fintech Research (Bank of Canada)

Ben Dovey (Bank of England)

Axel Kristinsson, Head of Department (Central Bank of Iceland)

Barbora Kalmaityte, Market Infrastructure Specialist (European Central Bank)

Herve Tourpe, Head of Digital Advisory (IMF)

Naoto Shimoda, Associate Director General (Bank of Japan)

Kjetil Watne, Special Adviser (Norges Bank)

Terje Åmås, Special Adviser (Norges Bank)

PBCDCI Team Digital Currency Institute (People's Bank of China)

P Vasudevan, Chief General Manager (Reserve Bank of India)

Sachin Sharma, Deputy General Manager (Reserve Bank of India)

Veljko Andrijasevic, Technology Expert (Sveriges Riksbank)

Mithra Sundberg, Head of the E-krona Division (Sveriges Riksbank)

David Lööv, Senior Economist (Sveriges Riksbank)

Ian Vitek, Security (Sveriges Riksbank)

Viktor Möllborg, Business Architect (Sveriges Riksbank)

Henrik Axelsson, Security Architect (Sveriges Riksbank)

Central banks who responded to the survey

Private sector & experts

Special acknowledgements to the individuals below, who were interviewed as part of this handbook, or for their insights, advice and feedback.

Amnon Samid, PE, Chief Executive Officer (BitMint)

Gideon Samid, PhD, Chief Technology Officer (BitMint)

Imran Khan, EVP Partnerships (Bitt)

Simon Chantry, Co-Founder and CIO (Bitt)

Joachim Samuelsson, CEO (Crunchfish AB)

Patrik Lindeberg, CEO (Crunchfish Digital Cash AB)

Andrew Marshman, Senior Account Executive (FIS Global)

Julia Demidova, Head of CBDC Product and Strategy (FIS Global)

Brett Walton, Head of Strategic Partnerships (Fluency)

Glenn Kim, MD, Strategic BD and Government Relations (Fluency)

Inga Mullins, CEO (Fluency)

Kamil Jamróz, Chief Architect, Aureum (Fluency)

Pawel Brataniec, CTO (Fluency)

Lars Hupel, Chief Evangelist CBDC (G+D)

Markus Bohn, Product Manager CBDC (G+D)

Polly Bäumler, Business Development Manager CBDC (G+D)

Raoul Herborg, Managing Director CBDC (G+D)

Severino Sequeira, Director Product Development CBDC (G+D)

Tanja Hessdörfer, Director of Sales and Business Development CBDC (G+D)

Teresa Riedl, Director Product Management CBDC (G+D)

Alexandre Fernandes, Sales Director (Giori Digital S.A.)

Jerome Ajdenbaum, VP Digital Currencies (Idemia)

Hugues Marie, Product Manager (Idemia)

Lauren Del Giudice, Senior Architect (Idemia)

Marten Nelson, CEO (M10 Networks)

Cizar Bachir Brahim, Chief Strategy Officer-CBDC Global Expansion (MetaMUI)

Phantom Seokgu Yun, Chief Executive Officer (MetaMUI)

Hiroto Masuda, Senior Specialist (NTT Data)

Shinji Setoriyama, Senior Manager (NTT Data)

Yoshiaki Wada, Senior Manager (NTT Data)

Yoshiharu Akahane, Decentralized Autonomous Society Strategist (NTT Data)

Anthony Ralphs, Director of Product Management CBDC (Ripple)

Antony Welfare, Senior Adviser CBDC and Global Partnerships (Ripple)

Bertrand Foing, CEO (Secretarium)

Cedric Wahl, CTO (Secretarium)

John Kiff, Research Director (Sovereign Official Digital Association)

Alain Martin, Head of payment systems consulting and CBDC lead (Thales)

Nicolas Le Cloirec, Payment systems consultant and CBDC project manager (Thales)

Amit Kumar Singh, Asst. General Manager - Business Expansion (ToneTag)

Rosa Giovanna Barresi, Lawyer, LLM, BABEL (University of Florence)

Catherin Gu, Head of CBDC and Protocols (Visa)

Mahdi Zamani, Director, Digital Currency Research (Visa)

Mike Gallaher, Senior Director, Government Engagement (Visa)

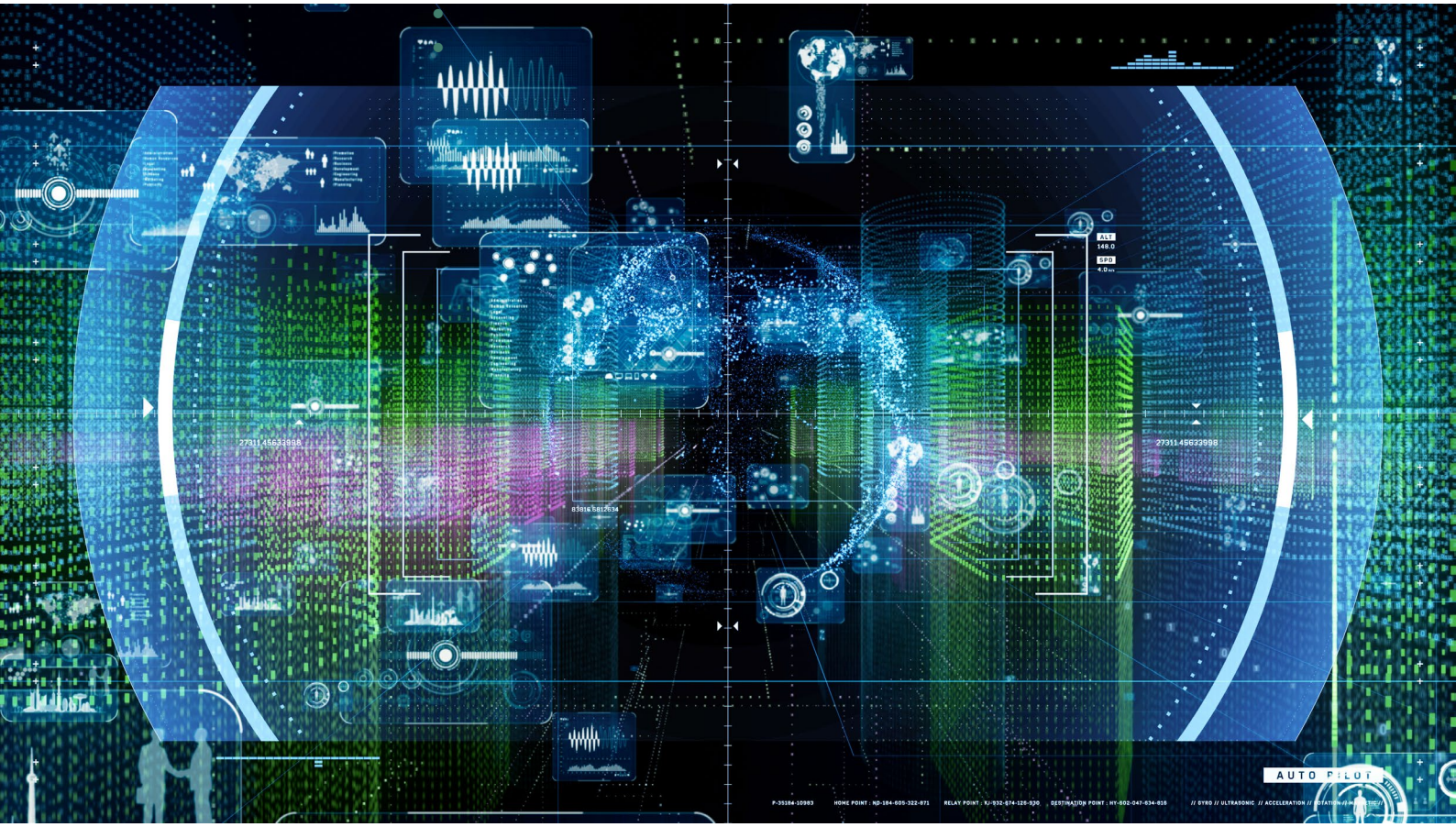
Stuart Smith, CBDC Product Manager (Visa)

Razvan Dragomirescu, Chief Technology Officer (WhisperCash)

Richard Turrin, expert and author

Special acknowledgements

Cecilia Skingsley, Ross Leckow, Dilan Olcer, Bénédicte Nolens, Raphael Auer, Miguel Diaz, Per von Zelowitz, Sonja Davidovic, Esther Rey Losada, Codruta Boar, Ben Dyson, Priscilla Koo Wilkens, David Whyte, Sameh Mikhail, Wipawadee Ayuporn, Jonathan Lee, Baltazar Rodriguez, Karen Martin, Andreas Adriano, Alan Soughley, Nora Fogelström, Hanna Wännlund, Åsa Staffansson, Malin Nyqvist.



ABC Annexes

Annex A: Further questions and considerations

This handbook has identified a number of further questions and considerations specific to offline payments with CBDC that could inform or have implications for the design of policy, system requirements, business requirements, operational management, change management, risk management and procurement. This annex describes each of the following main areas:

- Analysis, architecture and design
- Technology
- Security
- Operations and support
- Policy and processes
- Procurement
- User experience and payment acceptance

Under each of these sections is a set of questions that could be used as a guide for central bank staff across technology, business and policy roles to aid in the development of requirements for providing and supporting capabilities for offline payments with CBDC.

Analysis, architecture and design

Core

- What are the reasons for and different use cases to be addressed by offline payments functionality?
- What dimensions of inclusion are required (social, digital and financial)?
    - What are the requirements for each?
    - What types of solutions support these requirements?
    - What solutions are most accessible for those who may have physical or mental impairments?
    - What capabilities does a solution offer to support users who may have a physical or mental impairment?
    - What technology requirements does the solution place on users?
- What are the privacy requirements and trade-offs?
    - How do these requirements balance with compliance requirements?
    - What types of solutions support these requirements?

- What dimensions of resilience are required (short-term, ongoing and civil contingency)?
    - What are the requirements for each?
    - What types of solutions and modes of operation support these requirements?
- What are the conventions (eg other payment devices commonly used) and supporting infrastructure available in a country?
    - What types of solutions are more suitable?
    - Will more than one type of user device be required?
- How long should the selected offline payment solution continue to operate in the event of a major power failure or system or communication network outage, and what factors influence this?
- What trade-offs should be made, if any, between convenience and operational efficiency, user experience and risk management?
- What are the requirements for how an offline payment solution will need to support acceptance in all of the offline payment use cases required?
    - How does a solution achieve these requirements?
- What are the requirements for how an offline payment solution will be accepted alongside other common forms of electronic payment at merchants and for e-commerce?
    - How does a solution achieve these requirements?
- What are the requirements for how an offline payment solution will need to support person-to-person payments between different types of user device?
    - How does a solution achieve these requirements?

Architecture and design

- What are the operational resilience risks and dependencies associated with a given solution?
- Will a solution require customisation to meet the requirements of the central bank, and to what extent?
    - What are the change and operational management considerations associated with any customisation?
- What is the relative cost of deploying and operating different solutions, for example smartcards versus mobile applications?

Industry engagement, readiness and testing

- Which public- and private-sector actors will need to be engaged to implement offline payment capabilities?
- What are the plans for industry testing, pilots, staged rollout and full production operations?

Compliance

- What are the requirements to support compliance with AML/CFT regulations?
    - As offline payments cannot be monitored in real time or potentially at all, this could create a risk of abuse for illegal activities. How does a solution minimise the risk of breaching AML/CFT regulations?
    - What limits are required?
    - What is the requirement to maintain a record of offline transactions?
- What are the applicable national and international legal and regulatory frameworks that influence the design, implementation and operations of the CBDC system and offline payments?

Technology

General

- How does a solution deliver tamper resistance?
- Will the offline payment solution be separate from the online solution?
    - If separate, what are the integration requirements and dependencies?
    - If separate, will the offline payment capability be implemented at a later point?
- How should offline payment solutions allow for offline settlement?
- What modes of offline payment would best suit the range of requirements?
- Should the value transfer protocol be bidirectional or unidirectional?
- What value-form(s) would be most appropriate to meet various requirements?
- How does the value transfer protocol support functionality to help manage situations where value is lost during an offline payment transaction?
- In the case of hardware-based solutions, how is obsolescence managed?

Performance testing

- What are the performance, processing and scalability requirements?
- How will solutions be stress-tested to meet and exceed these requirements?
- Will testing include high volumes of low-value or micro transactions, throughput capacity and response times?
- What will solution vendors be expected to demonstrate and how?

- What testing is required to understand the limits to scalability and the costs associated with upscaling the system?

Interoperability

- What are the requirements for interoperability between the online and offline payment systems?
    - How does an offline payment solution enable this?
    - What are the implications for risk management?
    - What are the limitations?
- What are the requirements for interoperability between different offline payment solutions?
    - How does an offline payment solution achieve this?
    - How is a seamless user experience achieved?
    - What are the implications for risk management?
    - What are the limitations?

Future-proofing systems

Solutions need to support future-proofing of their systems. Most vendors have made allowance for this in their solutions, either through reissuance of cards or reprovisioning of mobile-based applications.

Future attacks

- Although solution vendors cannot mitigate all possible future issues, what strategies do they have to deal with new attacks or new faults?
- What capabilities exist or need to be established for central banks and their solution vendors to analyse, research, monitor and be ready to counter new threats and vulnerabilities?

Advances in technology

- What advances in technology need to be taken into consideration and potentially planned for?
    - For example, could developments in multi-access edge computing support offline payments by offloading processing from centralised components to those operating at the edge of a network? This may allow volumes of micropayments from IoT devices without overwhelming the capacity scalability of the system.
    - Another example is the use of physical unclonable functions,[54] where the user device itself is used to derive secrets using natural randomness that

[54] See Gao (2020).

can be used to mutually authenticate devices and protect payment transactions.

- What might be the threats and risks from advances in quantum computing?
- What are the threats from with A.I. assisted attacks?
- What ongoing research is required to support innovation in offline payments and against security threats?

Security

Cryptography

- What are the cryptography requirements for an offline payment solution?
    - How does the solution support crypto-agility?
    - How does the solution vendor ensure the appropriate level of crypto-durability and for how long?
    - Does the solution vendor use quantum-safe cryptography or can the solution be easily adapted when required?
- What is the FIPS cryptographic boundary to which modules on a user device have been certified?

Standards, assurance and certification

- What industry standards for security does a solution vendor use?
- What certifications does a solution vendor have?
- What security evaluations and ongoing testing and assurance will be required for offline payment solutions?
- How will value transfer protocols be analysed or evaluated by third parties to protect against certain threats, for example replaying a payment to the same device or redirecting a payment to another device?

Purse provisioning and life cycle management

- What are the requirements for secure provisioning of user devices?
- What facilities, systems and process are used by the solution vendor for secure provisioning and life cycle management?
- What due diligence, evaluation, assurance and certification will be required to be performed on the facilities and processes used by the solution vendor and their suppliers?
- How are keys securely generated and stored?

- How are provisioning requests initiated and associated to an end user?
- How will reprovisioning work?
    - How will any value stored on the previous device be retrieved and transferred to a new device?
    - What secure processes, risk assessments and assurance will be required for secure software solutions not based on secure elements or trusted execution environments?

Incident management

- What types of incidents does a solution vendor provide robust prevention measures for?
- What types of incidents can a solution vendor detect?
- What are the requirements for detecting and reacting to incidents?
- How does a solution vendor support the ability to detect an incident?
- What are the solution vendor's incident management processes?
- Will forensic analysis capabilities be required to investigate attacks on user devices or lost value?
    - How would this be provided and by whom?
- What risk management mechanisms are required to detect and react to breaches?
    - What mechanisms does a solution provide?
- What mechanisms are required to respond to and recover from attacks on offline payment systems?
    - What mechanisms does a solution provide?
- How will risk and incident management teams be prepared and able to respond to incidents where breaches of offline payment solutions occur?
- What are the robust and tested processes and systems that will need to be implemented to deal with such incidents?
- What suppliers is the solution vendor dependent on and how?
- What joint incident response training would be required?

Operations and support

- What are the operational functions and processes that would need to be established to support offline payments?
- What types of resources will be required to support offline payments across the organisation?

- What roles are required to operate the system and manage change?
    - What are the responsibilities of each role?
    - What identity and access management controls apply to a given role?
- What general and specific cyber security training will be required for each role or for the organisation as a whole?
- How will enterprise risk management processes need to be augmented to manage risks associated with offline payments?
- Should the operations for offline payments be outsourced or insourced?

Policy and processes

- What are the requirements for collecting and analysing transaction histories for offline payments?
- What are the requirements for monitoring accounts and offline payments with respect to compliance with AML/CFT and KYC/KYB obligations?
- What types of limits would be enforced and how?
- How often would user devices be required to connect online?
- How will the business models to support offline payments with CBDC need to be designed, for example to incentivise private-sector actors?
- What is the liability scheme that would need to be established for offline payments using CBDC?
- What policies would need to be established to support the management and replacement of lost value?
- Will a dispute resolution service be required to support offline payments?
- What technical certification services will be required for intermediaries, and who should provide this?
- What are the rules that would need to be established for user onboarding?
- What are the penalties for poor due diligence that results in onboarding a bad actor into the system?
- In the event of fraud, lost transactions, breach, counterfeiting, double-spending or other unfortunate event, who is liable and who underwrites the risk?
- What online features and functions, eg limits or remuneration (interest rates) apply to offline payments?

Procurement

- Who will be managing and delivering the implementation of the offline payment solution?

- Once in production, will the solutions be outsourced or operated in-house?
- What are the processes for managing new releases of software and/or hardware?
- What are the processes for managing necessary security patching and hotfixes?
- How will these be assured to the same level of security as existing deployments, and who will carry out assurance?
- What testing and acceptance processes are needed to make new versions of software or hardware operational?
- What service level agreements (SLAs) would be required with solution vendors?
- What is required from a solution vendor to ensure continued support and maintenance of contracts?
- Are escrow agreements required so the central bank can take ownership of software or hardware in the event that the vendor is unable to continue support?
    - How will updated software or hardware held in escrow be tested and updated?
    - Where solutions are dependent on third parties (for example, mobile phone manufacturers) how would escrow and testing arrangements need to work?
- How will the solution vendor manage incidents, often in partnership with the central bank?
- What level of visibility of the vendor's supply chains is required?
- How will a supply chain risk assessment be carried out, how often, and by whom?
- How will the solution vendor need to execute and support testing and pilots in order to reach operational readiness and production deployment?
- What is required of solution vendors to support localisation of services, for example supporting local languages for operator interfaces?
- How are risks underwritten by solution vendors – for example, is there liability insurance in place, and what types of risk are covered and to what level?
- How are issues escalated to the solution vendor?
    - How will critical issues need to be defined and responded to?
- What contractual terms are required?

User experience and payment acceptance

- What user groups that represent a "whole-of-society" view should be involved to ensure that CBDC systems supporting offline payments work for everyone?
- What user experience issues will need to be addressed?
- What are the common user experience principles that need to be established?

- How will the user experience be designed so that end users can pay seamlessly without having to know when they are online or offline?
    - How will online and offline balances be segregated?
    - Is it possible to make some amount available to spend offline automatically?
    - Could this be user-defined?
- How will users make sure they are paying the correct payee?
    - How will the risk of impersonation fraud be mitigated?
    - What implication does this have on privacy protection?
- How do solutions provide the ability to easily transfer value online and offline?
- How will users be assured and aware of the security of the solutions they are using?
- How will user experience need to support adoption of CBDC?
- How does the solution support acceptance in all of the offline payment use cases required?
- How will the offline payment solution be accepted alongside other common forms of electronic payment at merchants and for e-commerce?
- How will the offline payment solution support person-to-person payments between different types of user device?
- Does the solution have any capacity to allow users to share devices while maintaining their privacy?

Annex B: BIS survey of central banks on offline payments with CBDC

As part of the preparation of this handbook, the BIS Innovation Hub surveyed and interviewed central banks actively working on CBDC to obtain their views on offline payments with CBDC. The summary of statistics is detailed in this annex, and other findings and observations have been included earlier in the handbook.

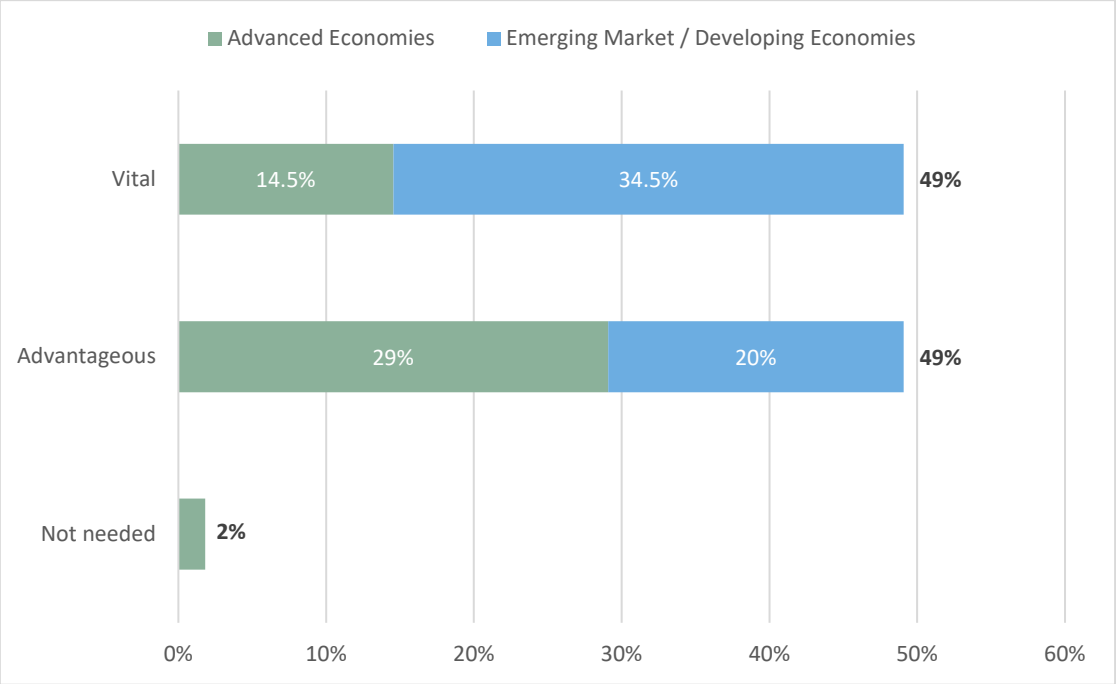
Fifty-five central banks representing 71% of the global population responded to the survey. Of the central banks surveyed, 47% are from advanced economies (AEs) and 53% are from emerging market and developing economies (EMDEs).

The results of the survey are detailed in this section.

Should offline payments with CBDC be possible?

Central banks consider the ability to make offline payments using CBDC an important feature, with 49% considering it to be vital (14.5% from AEs and 34.5% from EMDEs) and 49% considering it to be advantageous (29.1% from AEs and 20% from EMDEs).

Should offline payments with CBDC be possible? Graph 2



This graph shows both the fraction of total answers and how the answers differ between AEs and EMDEs.

Source: BIS IH central bank survey on offline payments with CBDC.

Graph 2 shows that EMDEs consider offline capability to be vital while AEs consider it advantageous. In particular, offline payments are more likely to be viewed as essential in countries where digital payment services are less developed or less accessible. Internet or mobile connectivity could be limited. In rural or disaster-prone areas, offline can provide critical services during temporary disruptions in power and internet services.

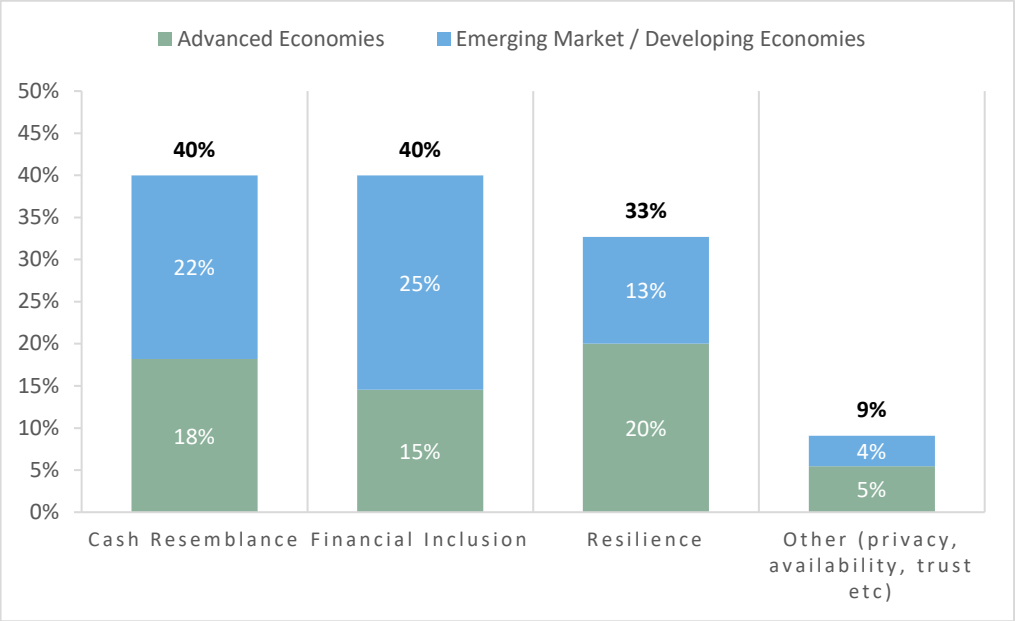
Despite considering offline functionality advantageous, a small number of central banks mentioned that its relevance may decrease in the future with further advances in telecommunication connectivity and satellite-based internet services, or that it is less important in areas with high financial accessibility and well-developed digital payment systems.

What are the main goals for offline CBDC?

The main goals for offline payments with CBDC cited by central banks are financial inclusion, cash resemblance and resilience. This is true for both AEs and EMDEs. Other reasons given included privacy, availability and trust.

The central banks surveyed cited several goals. A total of 40% cited financial inclusion as a goal (15% from AEs and 25% from EMDEs), 40% cited cash resemblance as a goal (18% from AEs and 22% from EMDEs), and 33% cited resilience as a goal (20% from AEs and 13% from EMDEs).

What are the main goals for offline CBDC? Graph 3



Survey respondents could select more than one option, so the total does not add up to 100%.

Source: BIS IH central bank survey on offline payments with CBDC.

Financial inclusion: Many central banks stated that offline payments with CBDC should be possible whenever technically feasible. The need for offline payments was especially important in countries where individuals use feature phones rather than smartphones and in areas without internet access and/or electricity. Some central banks stated that offline payments with CBDC should be available to unbanked users and for retail payments.

Cash resemblance: Many central banks believe that it is important that CBDCs and cash share some of the same user experience and features. Some say that user should be able to pay with CBDC held offline even when online systems is available, similar to cash payments.

Resilience: Some central banks took the view that offline CBDC was an important addition to the payment options available in their jurisdictions.

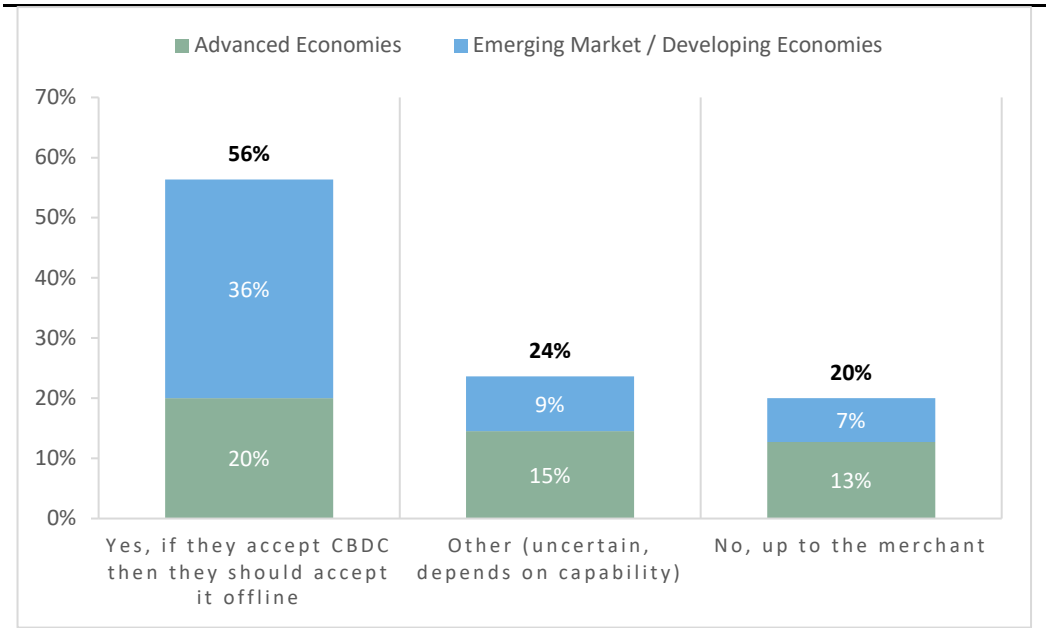
According to the survey, possible use cases for offline payments include power outages, areas without internet connectivity, and network connectivity issues. Several central banks said that offline CBDC requires periodic network and power connectivity to reload or redeem CBDC balances or to synchronise local wallet balances with central servers.

It is notable that different central banks had different approaches to the type of user device that would be deployed, particularly in respect of whether hardware- or software-based security would be used. The main basis for this difference appeared to be operational, in terms of what was practical in their jurisdictions given geography, demographics and existing infrastructure, rather than a purse security issue.

Should merchants accept offline CBDC payment?

Fifty-six per cent of central banks (20% of AEs and 36% of EMDEs) stated that merchants should accept offline CBDC, citing reasons such as acceptance, legal tender and user experience. Twenty per cent of central banks (13% of AEs and 7% of EMDEs) said it should be up to the merchant. Twenty-four per cent (15% of AEs and 9% of EMDEs) stated it would depend on architecture, technical complexity, or interoperability or that they were uncertain at this point.

Should merchants accept offline payments with CBDC? Graph 4



This graph shows both the fraction of total answers and how the answers differ between AEs and EMDEs.

Source: BIS IH central bank survey on offline payments with CBDC.

Requiring merchants to accept offline CBDC involves a number of issues that would need to be addressed:

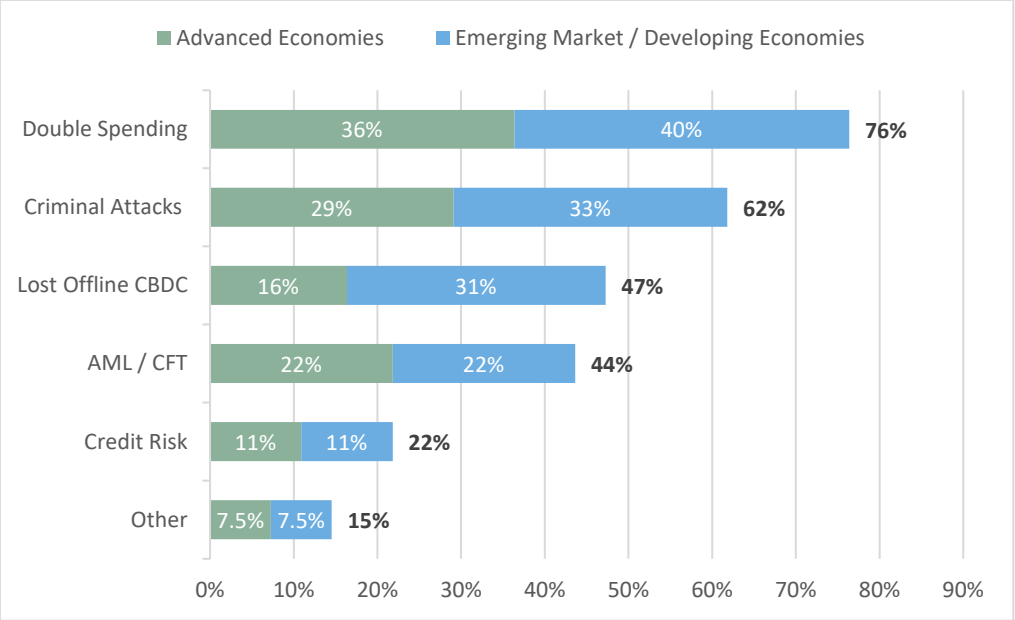
- the complexity of the technical implementation for acceptance infrastructure facilitating offline transactions;
- the value-form of CBDC that would be accepted;
- merchant and consumer expectations and protections related to offline payments are necessary for CBDC to be seen as important or useful enough to be accepted;
- support from merchant or custodian services;
- interoperability between online and offline systems (between the CBDC system and "last-mile" infrastructure); and
- application of transaction limits to mitigate risks such as double-spending.

What are the greatest risks with offline payments with CBDC?

Double-spending and criminal attacks were seen as the greatest risks associated with offline payments using CBDC, followed by risks related to lost CBDC and AML/CFT.

Both AEs and EMDEs seem to have a similar view on all risks except for lost CBDC, which EMDEs perceived as more important.

What are the greatest risks with offline payments with CBDC? Graph 5



Survey respondents could select more than one option, so the total does not add up to 100%.

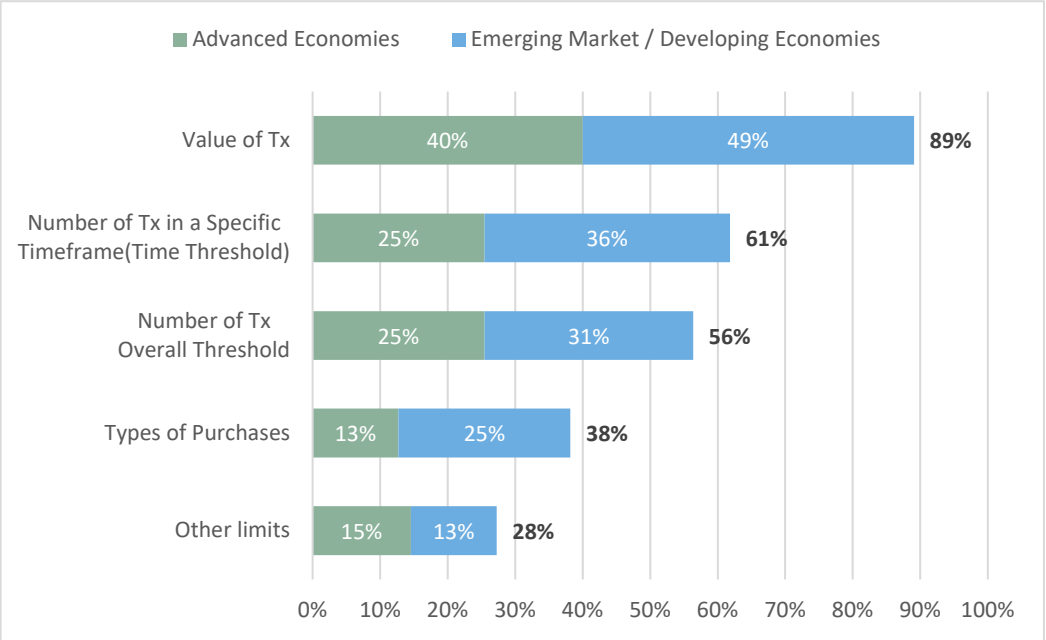
Source: BIS IH central bank survey on offline payments with CBDC.

What types of limits could be introduced to manage risks associated with offline payments with CBDC?

Central banks consider it important to apply limits to the offline use of CBDC in one or more ways in order to mitigate several risks associated with offline payments. There is a broad agreement on the relative importance of limits relating to the value and number of transactions. Type of purchase and other limits were viewed as less important, and the former would be difficult to implement.

What types of limits could be introduced to manage risks with offline payments with CBDC?

Graph 6



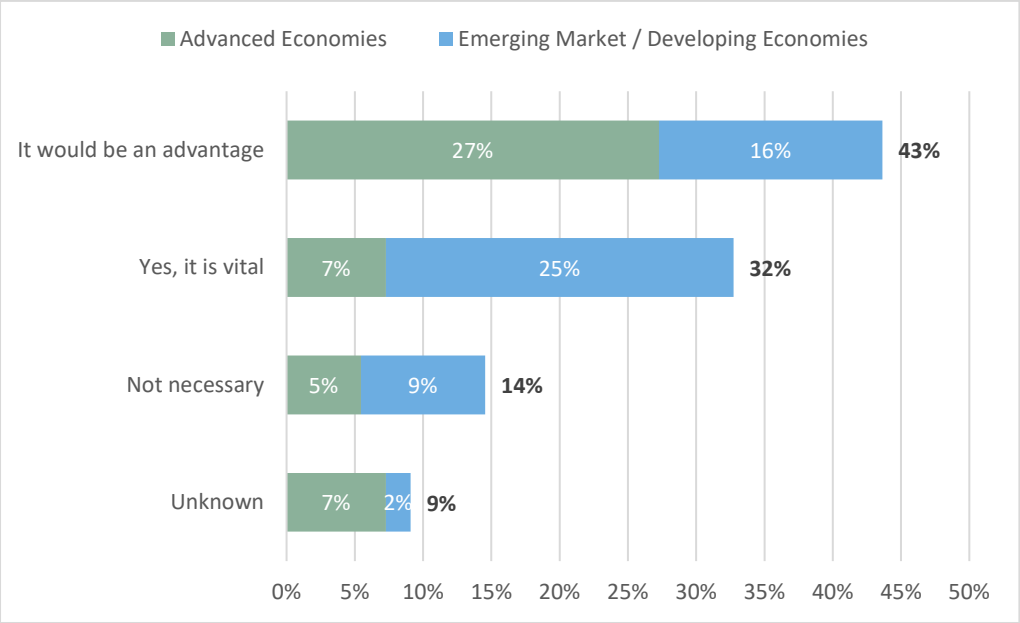
Survey respondents could select more than one option, so the total does not add up to 100%.

Source: BIS IH central bank survey on offline payments with CBDC.

Should it be possible to restore CBDC held offline?

Most central banks (77%) say that it is either vital or an advantage to be able to restore CBDC held offline. There is a general desire for the ability to restore lost transactions, but this is more important in EMDEs than in AEs.

Should it be possible to restore offline payments with CBDC? Graph 7



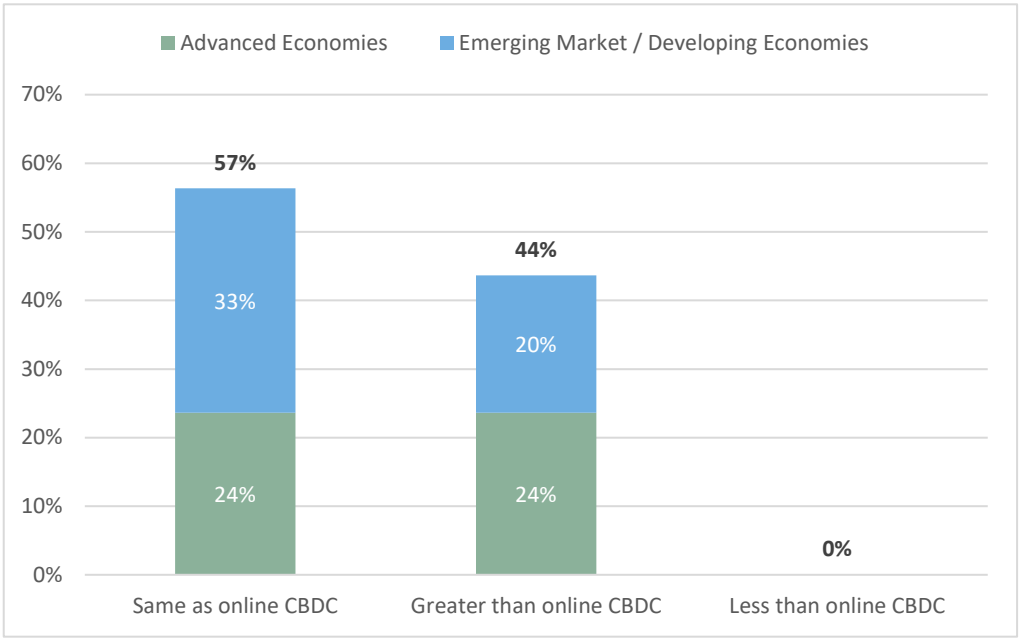
This graph shows both the fraction of total answers and how the answers differ between AEs and EMDEs.

Source: BIS IH central bank survey on offline payments with CBDC.

What level of privacy should apply to offline payments with CBDC?

All central banks surveyed said that the level of privacy should be either the same as or higher than for online payments with CBDC. No central bank said that the level of privacy should be lower.

What level of privacy should apply to offline payments with CBDC? Graph 9



This graph shows both the fraction of total answers and how the answers differ between AEs and EMDEs.
Source: BIS IH central bank survey on offline payments with CBDC.

Graph 9 shows that fifty-six per cent of central banks said the level of privacy should be the same as for online payments with CBDC (24% from AEs and 33% from EMDEs).

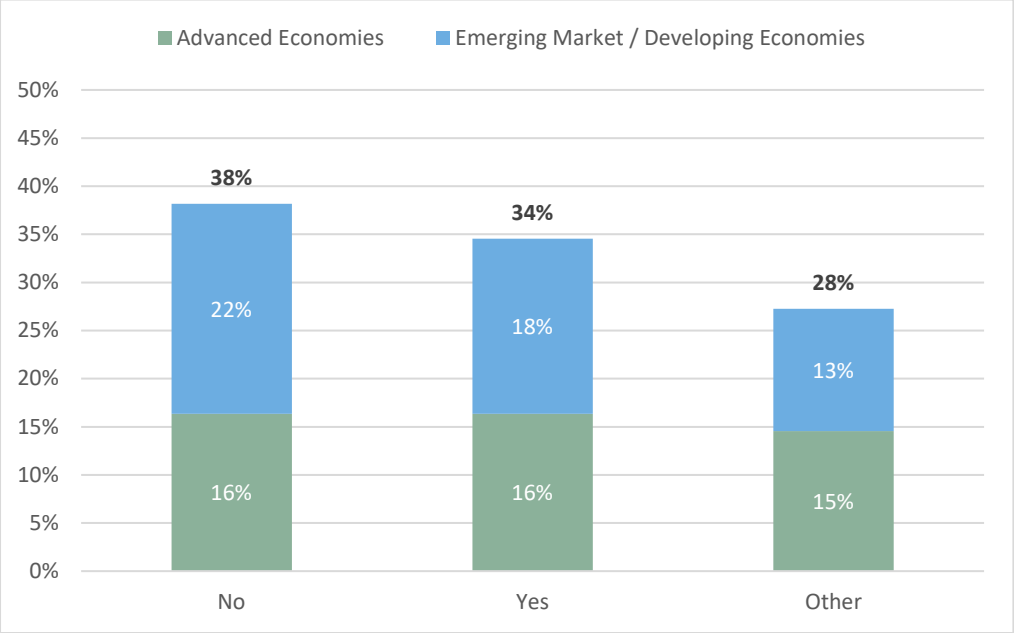
Forty-four per cent of central banks said the level of privacy should be greater than for online payments with CBDC (24% from AEs and 20% from EMDEs).

Offline CBDC can be an option for end users to initiate offline payments, even if online CBDC is an option. However, privacy protection needs to be balanced with compliance with AML/CFT and KYC/KYB rules. Offline payment solutions could become vectors for certain money laundering techniques such as smurfing.

Should offline payments with CBDC be used in cross-border payments?

Only 34% of central banks said that offline CBDC should be allowed to be used across borders (16% from AEs and 18% from EMDEs). There is no major difference between EMDEs and AEs.

Should offline payments with CBDC be used across borders? Graph 10



This graph shows both the fraction of total answers and how the answers differ between AEs and EMDEs.

Source: BIS IH central bank survey on offline payments with CBDC.

Typically, central banks' primary focus for offline payments with CBDC is domestic payments,

Many central banks stated there would be challenges in coordinating compatible solutions across jurisdictions, and there are certain dependencies on security and fraud controls.

Some central banks also stated that offline functionality could not be used for cross-border payments with CBDC.

Some central banks said that cross-border payments with offline CBDC could be possible with mutual agreement, but the cross-border policy of each jurisdiction would need to be addressed.

In practice, cross-border offline payments would be difficult to achieve, for example due to device compatibility and interoperability, how foreign exchange rates would be applied to transactions. It could be easier in single currency areas.

Annex C: A short history of offline payments

Introduction

This section presents the historical context of offline electronic payments, including many projects on which the authors of this paper worked directly. Strikingly, the technology challenges these projects faced remain largely unchanged, while many of the lessons learned from these projects are still relevant today:

- The commercial model is critical.
- Technology challenges can be overcome.
- Solutions must suit the local infrastructure and culture.
- User experience is important for adoption of new payment methods.

Solutions

The specific projects described in this section are:

- Digicash[55] – denominated digital coins
- Mondex[56] – unaccounted offline value
- Proton/Dancoin/Chipknip/Visa Cash – staged offline, accounted purses[57]
- EMV Offline – offline, but where value is not accounted for until the merchant goes online
- Transport for London contactless payments – only card verification is done at point of entry; payment value is calculated later and submitted at end of day, with risk of insufficient funds
- M-PESA[58] – not offline, but an interesting example of how mobile money over thin data channels can be very effective
- TAP – a solution using a mesh system to synchronise multiple offline devices with a central system to manage patchy connectivity

Electronic purse systems

The first "electronic purse" systems could, in principle, have been co-opted by central banks to serve as the basis of a CBDC, and at least one (Mondex) was specifically conceived as such. All of them relied on combinations of cryptography and tamper-

55 An overview of Digicash is given in Abrar (2014).

56 Stalder and Clement (1999) provide a good description of Mondex.

57 The common European electronic purses of the 1990s are reviewed in European Money Institute (1996).

58 For background on M-PESA, see Hughes and Lonie (2007).

resistant hardware to provide a major part of the protection of electronic value and anti-counterfeiting.

The fundamental issues that central banks wrestle with today applied equally to the electronic purse systems of the 1990s. Central to these is protection against double-spending, to which three approaches were taken:

- Accounted systems: In these, every transaction was accounted by ledger systems. Electronic purses could transact offline (with restrictions), but all transactions had to reach the central accounting system eventually in order to prevent double-spending.
- Coin-based systems: Digicash was the first system of this kind. It came closest to replicating metal coins and paper notes, with digital coins of fixed denomination. The payee could not confirm a coin's validity, so cryptographic value transfer protocols and accounting to online systems were adopted to prevent double-spending.
- Value-based systems: Mondex was the first system of this kind and was launched publicly. Value was distributed to purses (value stores) held on smartcards within the system, which could exchange value freely between themselves without reference to any central ledger system. Double-spending was prevented by tamper-resistant hardware and cryptographic value transfer protocols.

These systems were deployed in the early 1990s, with few surviving beyond 2000. There are some common threads in their history worth noting:

- At the time, cash was still the primary method for face-to-face transactions, and the electronic purse systems had few obvious advantages for most consumers and retailers.
- These offline payment methods were introduced just as the internet was becoming ubiquitous. Online payments rapidly superseded offline purses.
- By the late-1990s, the bank card industry had begun to use the hardware smartcard technology proven by the electronic purse projects to improve the security of credit and debit cards via the EMV protocol, which had also become the default way of paying for things online. Transaction costs were falling consistently, meaning that debit cards became viable for supporting the kinds of transactions for which electronic purses had been designed.

Accounted systems

Accounted systems relied on smartcards to physically protect value and cryptography to protect transactions. The earliest one was Danmønt (Denmark); other examples are Proton (Belgium) and Geldkarte (Germany). Geldkarte also provided a means of age verification at cigarette vending machines.

The Netherlands was unique in having two fully developed systems, Chipknip and Chipper.

The exception to the national orientation of these schemes was Visa Cash. Technically, Visa Cash was implemented differently in each country.

In practice, users of these systems held a limited portion of their bank account on their smartcard. Recipients of this electronic value – usually a merchant – could not pass any of it onto another party until the transaction had been reconciled by the recipient's bank.

Coin-based systems

Digicash was the earliest electronic purse system. It was based on a system of electronic coins of fixed denominations, much like physical cash, so in order to make a transaction, a set of coins was transferred. If appropriate, change could be given in the form of coins.

Its main innovation was cryptographic "blinding" for the purpose of anonymising transactions, even for the bank. Any user can create a coin. For that coin to have value, it must be cryptographically signed by the bank after its creator's account has been debited. The data representing the coin are blinded (encrypted) by its creator and then signed by the bank. These blinded, signed data are used to generate a signature over the unblinded coin data, which demonstrate that it originates with the bank without requiring access to the bank's private key.

At this stage, the creator can spend the coin, offline if necessary. However, for Digicash, verification of the signature on the spent coin could only be provided by the bank. In theory, the receiver of the coin could re-spend it before going online to the bank, but the receiver could not be certain of its validity. Once the coin was verified by the bank, it was cancelled.

Unlike accounted and value-based systems, Digicash did not require secure hardware, which was expensive at the time. Coin creators had to protect their (signed) coins before spending in case someone else copied them and spent the copy first. However, they could choose the degree of protection they applied.

Value-based systems

Mondex was designed as a global multicurrency scheme, and some central banks were involved as soon as the specification was mature. A core design principle was to make it as similar to cash as possible while aiming for the highest possible levels of security.

All value was held in secure hardware running the Mondex app, no matter the country or the type of purse holder (eg bank, merchant or consumer). However, there were many configuration options, mainly for security purposes.

All value was created by an "Originator", with only one Originator permitted for each currency. In practice, this was a joint venture between the Mondex member banks operating in the relevant currency area, with the expectation that the central bank would eventually take over. Value was created in a special Originator purse, which had normal Mondex functionality but which was created with a non-zero value, in a facility with security equivalent to that of a banknote printer.

The Originator purse would distribute value into the commercial banks' Mondex purses (against a movement of funds), which would then distribute it into consumer Mondex purses. A consumer purse could hold value in up to five currencies at once in configurable "pockets".

Mondex was fully offline, with no need for an associated bank account. Purses could acquire value from any other Mondex purse, with payment for the value (if any) at their discretion. Similarly, they could spend that value, in any amount, entirely offline. Some kind of electrical contact was required between the two interacting purses, but no contact with any kind of "official" purse or system was necessary.

Consequently, purse holders were exposed to losing value if they lost their card. It would not be possible to reconstitute value by examining a shadow account. If a Mondex transaction were interrupted (say because of an empty battery), the transaction would be completed if the two purses were reconnected, even if other transactions had since occurred on either or both purses, provided that the transaction had not expired from a circular transaction log on either card.

Other risks could be mitigated by configuring parameters associated with each currency, for example maximum stored value and maximum transaction size.

Due to the lack of a central authority, the value transfer protocol was complicated. Firstly, the currency and security version had to be agreed. The next step was to swap and validate the keys to be used in transactions. Then, a three-phase, fully signed and verified protocol was used for the exchange itself.

Mondex was trialled in many places including the United Kingdom, United States, Canada and Hong Kong. The last of these, in Taiwan, closed in 2008.

Phone-based initiatives

M-PESA (Kenya)

M-PESA, the mobile money system, has its origins in a system for the disbursement of microfinance loans. The system's designers constructed the payments infrastructure to be perfectly general and not restricted to that particular use.

It was soft-launched in Kenya in 2007, a year of great upheaval. Many Kenyans in rural areas chose to convert cash to M-PESA value for safekeeping. Thereafter, M-PESA became a common way for migrant workers in the cities to remit money to their families in the countryside. M-PESA has since gone from strength to strength, with more than 51 million customers across Kenya, Tanzania, Mozambique, the Democratic Republic of the Congo, Lesotho, Ghana and Egypt.

M-PESA is a peer-to-peer payment system. Transactions are carried out through the exchange of cryptograms over SMS from the payer's and payee's mobile phones via a central server that applies debits and credits to the ledger. Any mobile phone that supports SMS can support the service. The secure software is a SIM Toolkit application. This can require a user's existing SIM to be replaced by a new one.

Technically, M-PESA is an online service. However, SMS does not guarantee instant delivery, so in practice participating mobile phones may not have connectivity for a certain amount of time while a transaction is being completed.

TAP (Nigeria)

TAP was a system deployed in Nigeria which registered farmers qualifying for aid disbursements (to buy agricultural inputs such as fertilizer), prepared vouchers allocated to those farmers, and redeemed the vouchers at agricultural merchants.

A pilot system was trialled in two states, covering approximately 500,000 farmers over two growing seasons. It was necessary to carry out all phases of the service (registration, allocation and redemption) during intensive phases, according to the season. Most farms and most markets did not have reliable mobile network coverage.

The system relied on field officers carrying inexpensive tablets to remote locations. The camera was used to capture facial images of the farmer and a suitable identity document, along with information pertaining to the farm, for example which crops were to be planted. The farmer was issued a very simple smart memory card, which served solely to provide a unique identifier and was tapped against the tablet to capture the identifier via its NFC interface. The field officer returned to base with the tablet containing all the captured information for that day. Frequently, that base would not have mobile network coverage. The tablet NFC interface would be used to transfer all the records to a single device, which would be taken to a head office that did have coverage. Those records would then be uploaded onto a cloud server.

After validating the captured records, the server would attach vouchers to each farmer's records. Then the farmer's records were distributed to the farmer's local merchants. The distribution mechanism was exactly the reverse of the enrolment mechanism, utilising the NFC capability of the tablets in a chain-like fashion.

The farmer could then buy fertilizer by presenting his or her card at the merchant's tablet, which enabled verification of which vouchers could be applied against the purchase.

The system achieved a very high number of authentic transactions, much greater than a previous system based on paper vouchers had. Although funding could not be sustained, similar systems are now in place in other parts of Africa.

EMV Offline

The existing EMV protocol, used today in all Chip & PIN transactions, includes the concept of offline payments because it was developed before networks were pervasive. Although it is not used very often today, offline payments remain a part of the protocol and specifications.

Online transactions

The core elements of an EMV card are a transaction counter and a unique secret key known only to the card and the card issuer. For each transaction, the transaction counter is incremented and a cryptogram is calculated over the data sent to the card from the terminal, together with internal card data and the transaction counter. In this way, every cryptogram is different, even if the terminal data are the same. The transaction data plus the cryptogram are sent online to the card issuer for authorisation. The card issuer calculates a cryptogram using its knowledge of the secret key, and if the values match then the card issuer knows that the cryptogram came from their card and the transaction details are unaltered. The card issuer then approves the transaction and notifies the terminal.

The need for offline transactions

EMV was originally devised in an era where telecommunications costs in Europe were still high and networks were slow and unreliable. In many cases, especially for low-value transactions, the overhead of an online authorisation outweighed the benefit of establishing that the card was genuine and the amount was available to be spent. Consequently, EMV provides a mechanism to permit a card to approve a transaction offline and for the terminal to trust that decision.

The card must be balance-aware (ie must know how much spend is available to be approved offline). Two forms of offline spend are supported:

- **Preauthorised debit**, where an amount is allocated to the card and can be spent up to that limit before the card must go online. After any online transaction is approved, the available spend is reset to that preauthorised limit.
- **Prepay**, where the card tracks the cumulative amount spent and an ever-increasing limit represents the total permitted spend of the card. The available spend is the difference between the accumulated spend and the limit. Funds are topped up at the end of an online transaction by the issuer instructing the card to increase the value of the limit.

The mechanisms supporting offline transactions

A number of mechanisms are included in EMV to support offline transactions:

- Risk management, using floor limits in the terminal, offline spend accumulators and spend limits on the card, additional counters and limits on the card to restrict the number of offline transactions, and cryptographically protected responses to indicate that the card has approved the transaction.
- Offline data authentication, to allow the terminal to establish that the card is genuine using PKI technology.
- Cardholder verification, to establish that the card is being used by the genuine cardholder. Two methods are available to support this: Offline PIN and Consumer Device CVM. When an offline CVM is successful, an indicator is set in the card's internal data and included in the cryptogram calculation for the card issuer. An

indicator is also returned to the terminal; however, this may not be covered by the card's offline digital signature.

There are some risks associated with offline cards which never go online, eg the ability to continue to spend to the offline limit even after the card has been reported lost or stolen and the account has been blocked.

These risks are managed to an extent by expiry dates and terminal block lists. This (coupled with significantly lower telecommunications costs) has led payment brands to mandate zero-floor limits in most cases, although offline data authentication is still used to prove that the card is genuine.

As network connectivity has improved, and particularly with the increased use of contactless transactions (where there is no provision for issuer management of cards), usage of offline EMV has dropped significantly. For commercial banks and payment schemes, this makes financial sense as it reduces the risk associated with offline payments. However, it also limits the use cases supported by payment card products.

Contactless payments in transit

Transport for London (TfL) was the first mass transit operator to introduce contactless payments using standard payment cards for access to its network. Due to the exacting nature of the mass transit environment, this was implemented as a form of delayed authorisation using aspects of offline payments. This model has now rolled out to many other transit operators across the world.

TfL launched its Oyster card in 2003. This is a "closed loop" payment system, which was popular with customers – by 2012, 80% of public transport journeys in London used an Oyster card. The main drawback for TfL was that the cost of running the Oyster scheme amounted to about 14% of the fares collected.

Therefore, from 2008, TfL began to investigate alternatives, specifically the use of contactless debit and credit cards using the EMV standard, in order to reduce the cost of revenue collection and provide customers with an easy-to-access payment method. A critical requirement is that transactions at transit gates be quick, because if not, queues build up at ticketing gates, rapidly causing safety issues.

There are two main problems for EMV transactions in this environment. Firstly, it cannot be guaranteed that readers are always online, especially on buses. Secondly, even if fully online at a reasonable data rate, most authorisations will take longer than could be safely allowed.

This problem was solved by dividing the transaction into two parts. Firstly, a local reader determines if a card has been validly produced by a member of a recognised scheme, such as Visa or Mastercard. A check against a locally held deny list prevents the use of cards reported as lost/stolen as well as cards not in good standing. At this point, if these local checks are passed, the gate will open, and the passenger enters the rail system or the bus.

Next, an authorisation request is submitted through the card scheme to the card issuer for a nominal amount, as the ultimate charge is not known until the rider exits the system or later. Should the authorisation be declined, the transit operator can add the card to the deny list maintained at readers for future use. When "tapping out" of the system, a passenger whose card has been declined will be let out (for safety reasons). However, should they attempt to re-enter the system before their account has returned to good standing, they will be denied entry.

A back-office system keeps track of a particular card's journeys during the day. Based on usage and subject to the specific transit operator's and card scheme's rules, a financial transaction is then completed though the card network.

As these processes did not fit into the existing EMV fraud management models, they needed to be modified, but fraud rates have remained low across the many transit schemes that have implemented them around the world.

In pre-pandemic London, approximately 2.5 million contactless payments occurred in the system on an average day. Importantly, TfL met its original objective: the cost of distribution has fallen from 14% to 7% of fare revenue, even though the Oyster system still operates in parallel.[59] Based on this success, the system has been replicated in many major cities worldwide, for example New York and Sydney.

Lessons from historical solutions

These historical examples provide a number of lessons for offline CBDC:

- Security principles do not change – tamper-resistant user devices and cryptographic protocols allowing devices to exchange representation of value over secure value transfer protocols are enduring requirements.
- Risks do not change – double-spending and counterfeiting of value remain issues. It is essential to detect situations where value is lost in transit and needs to be recovered or otherwise accounted for (or it be assumed that the value was lost forever).
- Operational processes may need to adapt to new challenges: the master cryptographic keys that protect the payment processes need to be kept secure. However, the availability of mobile computing devices now means that payment applications may be provisioned while in the user's hand. This is a new issue that was never faced in historical systems.
- User experience: at the time most of these solutions were deployed the ability to make the user experience better than the alternative of cash was limited. For example, contactless solutions had yet to be deployed and the smartphone had not been invented. In more recent years, the successful adoption of PIX, the

[59] Although TfL does not publish this directly, this was confirmed in a response to a UK Freedom of Information request in 2022 – see tfl.gov.uk/corporate/transparency/freedom-of-information/foi-request-detail?referenceId=FOI-0141-2223.

smartphone based instant payment solution available in Brazil, highlights the importance of user experience in achieving adoption of new payment methods.

- Commercial model: many historical offline payment solutions struggled to offer a commercial model that solved the problem of attracting both payers (mainly individuals) and payees (mainly merchants) and generating enough value to make it worthwhile for intermediaries to support them. This could be an important consideration when introducing offline payments with CBDC.
- None of these systems went on to achieve population-scale success, apart from EMV and M-PESA, which are both largely online systems. In general, it is extremely hard to establish a new payment solution without a "killer" application that makes it essential for users. There is also significant competition from existing payment solutions, especially credit and debit cards, which the issuing banks, who were also the owners of many of the offline payment solutions, are strongly incentivised to promote.

Overall, the technical challenges and solutions faced by historical offline payment solutions remain similar today. For any solution – including a CBDC – to be adopted, it is essential that all parties in the distribution chain be competitively incentivised to promote and manage the solution.

Bank for International Settlements (BIS)

ISBN 978-92-9259-652-1