BIS Innovation Hub

Project Polaris

Part 4: A high-level design guide for offline payments with CBDC

October 2023

Contents

Executive summary

The design and implementation of offline payments capabilities for CBDC systems is a complex undertaking. Some challenges and trade-offs cannot be solved easily, despite the work of many central banks and private sector participants. Further, since each jurisdiction has unique requirements, there is no one-size-fits-all solution.

The BIS Innovation Hub (BISIH) previously published a handbook for offline payments with CBDC which provides a comprehensive overview of offline payments with CBDC.[1] The present guide is for central banks that have used the offline handbook to build their knowledge and now want to focus more deeply on their requirements and design choices for offline payments with CBDC.

The guide is based on information gathered in a series of deep-dive workshops conducted across May and September 2023 in collaboration with solution vendors and central banks. These workshops have provided a greater understanding of the current solution landscape and the design choices central banks need to consider when thinking about offline payment capabilities. The guide provides central banks with an approach to mapping their objectives onto their design choices. The guide ends with a number of illustrative scenarios that demonstrate how a central bank could apply the information contained in this guide to their own context.

The deep-dive workshops **reinforced many of the conclusions from the handbook**:

Providing offline payments with CBDC is an important requirement for many central banks. The drivers for offline payments with CBDC vary by jurisdiction. Some common motivations are supporting inclusion, offering cash-like features such as enhanced privacy, and increasing payment system resilience by providing an alternative option in the event of disruption.

Design choices must consider requirements for the whole solution. An offline payment solution cannot be designed in isolation. Some of the core links between objectives, characteristics and design options are shown in Graph 1. There are likely to be more links than those shown. **Trade-offs will exist between different requirements**. To overcome this, **central banks can take an iterative approach to design**, exploring alternative ways to achieve their objectives.[2]

The deep-dive workshops also **provided several additional conclusions**:

The overall maturity of offline CBDC payment solutions is evolving: very few are in a live environment working at scale. Solution vendors face common challenges

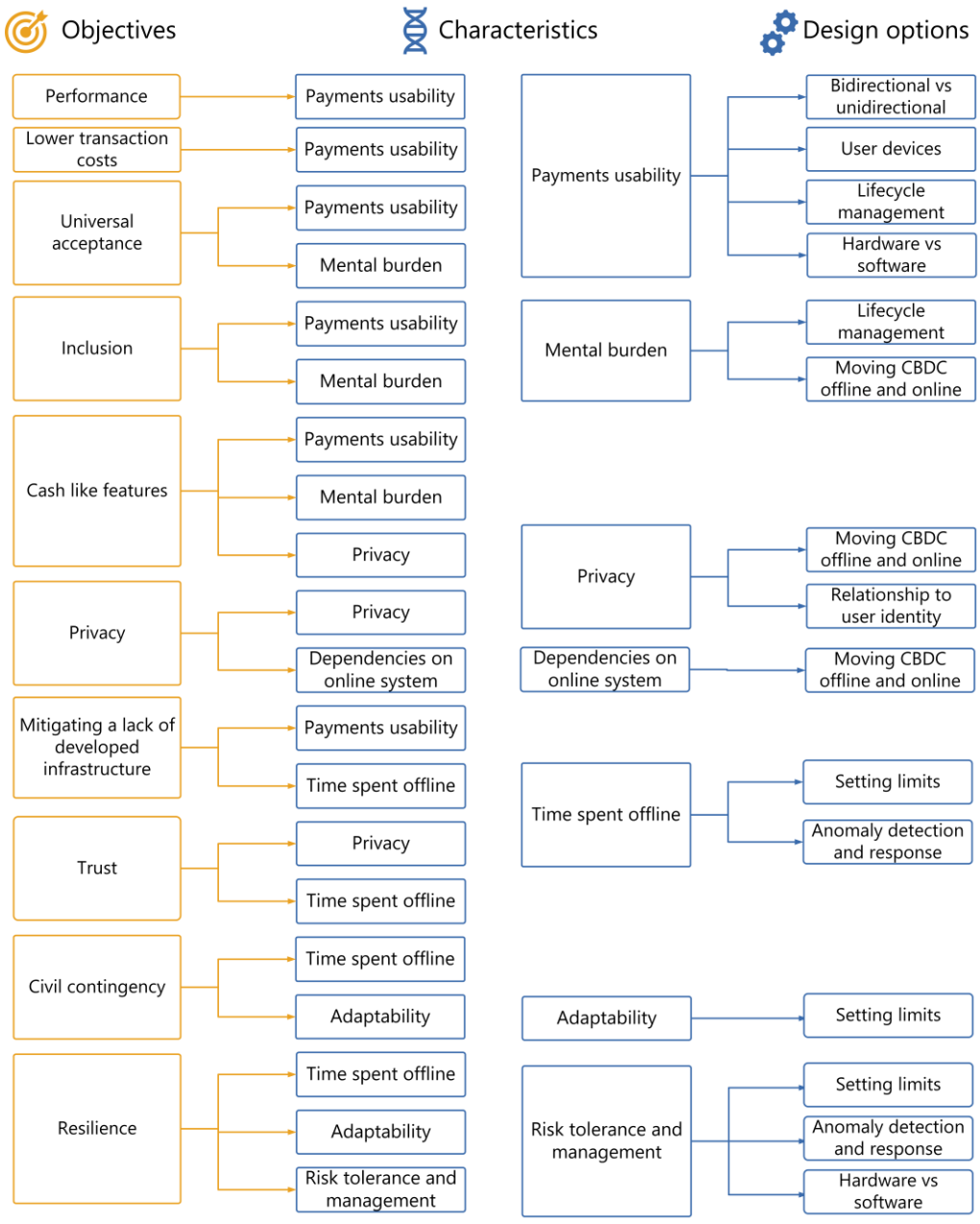
[1] See BIS Innovation Hub (2023a).

[2] Experimentation and iteration can lead to occasional failures. This is a risk central banks should be aware of and which should be balanced against the benefits of this approach.

in demonstrating they can **meet central banks' requirements** and ensuring that they have **sufficient funding** to continue their development.

For offline payments with CBDC, central banks can be a driving force for collaboration and innovation. They need to understand their context, determine their objectives and use these to define their requirements. By taking a leading role, central banks can support solution vendors in overcoming the challenges discussed above and ensuring **that solutions are based on their requirements, rather than on whatever technology is available**. This should be an iterative conversation. Only with a clear set of requirements can a solution vendor meet the needs of central banks. At the same time, central banks need to form an understanding of existing technology options to see what is currently feasible and where gaps remain.

Core links between objectives, characteristics and design options — Graph 1



Acronyms and abbreviations

AML	Anti-money laundering
App	Application
BIS	Bank for International Settlements
BISIH	Bank for International Settlements Innovation Hub
BLE	Bluetooth low energy
CBDC	Central bank digital currency
CTF	Counter-terrorist financing
EMV	Europay, Mastercard and Visa – the standard governing the majority of payment cards globally
IT	Information technology
KYC	Know your customer
NFC	Near-field communications
P2B	Person-to-business
P2P	Person-to-person
POS	Point of sale
PUF	Physical unclonable function
QR	Quick-response code
SE	Secure element
TEE	Trusted execution environment

1. Introduction

An offline payment with CBDC is defined as a transfer of retail CBDC value between devices where those devices do not require a connection to any ledger system, often in the absence of internet or telecoms connectivity.[3]

A small but growing number of offline payment solutions are being developed by the private sector that can potentially be used for CBDC.[4] The maturity and scale of these solutions vary. All of the solution vendors have highlighted the variety of complex challenges that are faced when developing an offline payments solution.

Different central banks will have different requirements for offline payments with CBDC based on their domestic context, technology strategy and policy needs. This means there is no one-size-fits-all approach. It is likely that there would be some core central bank requirements that are non-negotiable that solution vendors would need to adhere to. Beyond that, there may be trade-offs that would need to be carefully understood and balanced, covering the management of security and risk, achieving the desired policy goals, offering value to end users, creating a seamless user experience and meeting expectations and requirements for privacy.

The BISIH's previously published handbook for offline payments with CBDC provided a comprehensive overview of offline payments with CBDC.[5] A number of stakeholders found that the offline handbook has greatly increased their knowledge and understanding within a complex area of CBDC system design.

The guide is standalone, building on a number of foundational concepts from the offline handbook such as the most common central bank objectives for offline payments with CBDC, the modes of offline payment, the logical architecture for offline payments and other aspects of design including tamper resistance, lifecycle management and integration with an online system.

This guide has a specific focus on deepening central bank understanding of the technology landscape and discusses solution categorisation, design choices and central bank requirements. It also sets out an approach to mapping central bank objectives for offline payments with CBDC onto the design choices required to outline an offline payment solution. The full scope of the offline handbook and the focus of the guide is further detailed in Annex B.

The information within this guide is based primarily on a series of deep-dive workshops, which provided a detailed understanding of the current solution landscape and the design choices available to central banks considering an offline payment solution. Graph 2 shows an overview of the approach taken. The workshops

---

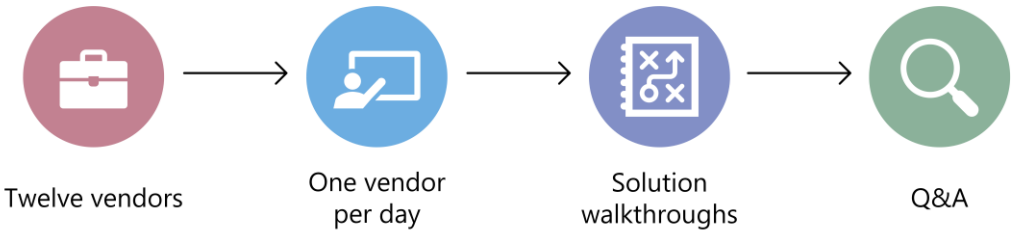
[3] This does not exclude the possibility that the offline devices may have online connectivity, but their users may choose to conduct an offline payment device to device.

[4] The origins of many, but not all, of these solutions predate CBDC requirements.

[5] See BIS Innovation Hub (2023a).

were organised over several weeks during May and September 2023. One solution vendor was invited to present each day, during which they would walk through their solution and engage in discussions with the BISIH, an external consultancy, and observing central bank participants. In total, 12 solution vendors participated in the deep-dive process.[6] This guide also draws material from other work undertaken on offline payments, both for CBDC and non-CBDC use cases.

Deep-dive workshop approach Graph 2



The design guide is structured as follows:

Chapter 2: The current offline CBDC landscape. This will consider the objectives and motivations of central banks, how the current solution and technology landscape can be categorised and the common challenges that solution vendors face.

Chapter 3: Design choices for offline payment solutions. Several key design choices shape an offline payment solution. These are interrelated and there is ample scope for trade-offs between different choices.

Chapter 4: Applying the design choices. Illustrative examples and guidance illustrate how to make use of the design choices, showing how a jurisdiction's unique context and objectives determine the relevant design choices.

Much of the technology being discussed could be applied elsewhere. Some of the solution vendors involved in the deep-dive sessions are applying their solutions or their technology in the space of identity, payments with commercial bank money or in wallets and infrastructure for regulated stablecoins.

[6] Observing central banks, external consultancy and participating solution vendors are shown in the acknowledgements. An open invitation was followed by a selection process to choose solution vendors for the workshops. The number of solution vendors interviewed was limited by time constraints and the availability of solution vendor representatives. At a minimum, solution vendors had to have implemented a prototype of their solution. A range of solution vendors were invited to ensure a variety of different potential solutions could be viewed during the deep-dive. The inclusion of any specific solution vendor should not be taken as an endorsement of their products, while the exclusion of any solution vendor does not indicate any issues with their solutions. Some invited solution vendors were unable to participate.

2. The current offline CBDC landscape

Development of offline payment solutions should be based on a collaboration between the public and private sector.[7] Central banks need to understand their context and their requirements for providing offline payment capabilities. The offline handbook provided various dimensions to consider when defining these.

Solution vendors need to understand central bank requirements and show how their solutions and expertise meet those needs. Central banks can leverage the comparative advantage of the private sector in building out technically complex user-facing solutions. Graph 3 highlights the considerations for both sides.

Without such collaboration, central bank requirements may not be met, and solution vendors may struggle to gain funding to continue their research and development. A central bank should consider collaborating with a broad range of stakeholders. This could include end users, merchants and financial service providers.

Central bank objectives and the solution landscape represent the two sides that need to be brought together to create an offline payment solution design. Chapters 3 and 4 demonstrate how to link these two aspects.

Central bank context and solutions considerations — Graph 3

2.1 Central bank objectives

The BISIH carried out a survey of central banks to obtain their views on offline payments with CBDC.[8] Graph 4 shows the primary motivations for a central bank to provide offline payment capabilities.

[7] See Bank for International Settlements et al (2021).

[8] See Annex A of BIS Innovation Hub (2023a).

Inclusion has multiple aspects all of which are relevant to central banks and offline payments with CBDC.[9] **Digital inclusion** provides people with the tools and skills to engage with digital systems. **Financial inclusion** enables people to exercise financial self-determination and access financial services. **Social inclusion** enables people to play an active role in society.[10] Often one inclusion challenge can aggravate another.[11] For example, someone who is digitally excluded and has no internet access may also be unable to access internet banking and other digitised financial services.

As a digital form of central bank money, offline CBDC could be designed with **cash-like features**.[12] For example, a private peer-to-peer payment with no external connection is similar to exchanging a banknote.[13] This may be relevant in jurisdictions where cash usage is declining but there is no clear digital alternative.

Offline CBDC could offer an additional **resilience** layer by acting as a payment option in the event of outages in the online CBDC system, other payments systems or the network infrastructure. It may also provide resilience where online connectivity is poor or intermittent. As digital payments become more prevalent and dominant in some jurisdictions, this increases the need for a backup in the event of an outage.[14]

Primary motivations for offline payments with CBDC — Graph 4

Inclusion, cash-like features and resilience are the objectives most commonly referred to by central banks. The order of other objectives does not necessarily reflect their relative importance

Objectives should determine requirements, which should determine solution design. A solution for one central bank may not work for another, as different objectives may create different requirements. Central banks should avoid the common design mistake of selecting a specific solution before requirements have been elaborated.

9 See eg Minwalla et al (2023).

10 See Chapter 7 of BIS Innovation Hub (2023a).

11 See eg Hayashi and Minhas (2018).

12 Central banks should be clear on which features of cash they want to replicate. For example, cash is both a store of value and a means of payment, but these features could lead to quite different design choices.

13 See eg European Central Bank (2022).

14 See eg Sveriges Riksbank (2022b).

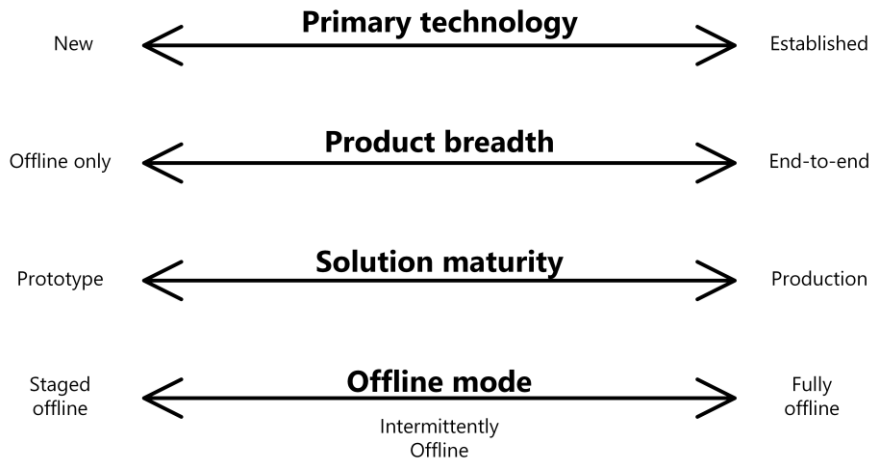
2.2 Current technology landscape and challenges

The specifics of each solution are unique, but they can all be described in high-level terms based on four categorisations. These are their primary underlying technology, the breadth of their product, the maturity of their solution and their offline mode.

All solution vendors share some common challenges in demonstrating how they can meet central banks' requirements and how they can get the necessary investment to continue developing their solutions.

2.2.1 Categorising the current technology landscape

Four criteria to categorise the current technology landscape — Graph 5



Graph 5 shows the four criteria that can be used to categorise the different technology approaches for offline payment solutions, as described in Table 1. They are based on information gathered from solution vendors as part of the deep-dive workshops and build on categorisations established in the offline handbook such as the mode of offline payments.[15]

Description of the four criteria categorising the current technology landscape — Table 1

Criteria	Description
Primary technology	Many solutions rely on technologies that have existed for several years, for example smart cards.[16] This technology is well understood but was not designed specifically for offline payments with CBDC. Some solution vendors are exploring new or novel technologies in their solutions. Some of these could be more tailored to central bank requirements but their scalability and operational readiness could also be more challenging to prove, as discussed in Section 2.2.2.

[15] See Chapter 3 of BIS Innovation Hub (2023a).

[16] See Annex C of BIS Innovation Hub (2023a).

Product breadth	Some solution vendors offer an end-to-end CBDC solution, of which offline payments with CBDC is one aspect. Other solution vendors only offer the offline payments solution, which they suggest can be integrated into an online solution. In both cases, the offline system will have dependencies on an online system. More detailed aspects of the product offering, such as the security approach, is discussed as part of the design choices in Chapter 3.
Solution maturity	The overall maturity of solutions continues to evolve. Currently there are very few offline solutions for CBDC that are production-ready or working at scale in a live environment. That said, there are a number of mature pilots, with solution vendors already actively working with central banks. Other solutions could be characterised as prototypes and proofs of concept. Solution maturity should consider several aspects including operational readiness, crypto-agility, solution vendor capability and user experience.
Offline mode	The mode of offline payments determines the approach taken to onward spending of CBDC held offline. For ease, three modes are assumed: • **Fully offline** is where value that has been exchanged from a payer to a payee can be spent again immediately and indefinitely. There is no requirement for connecting back to the online system. • **Intermittently offline** is similar to fully offline but at set risk management or technological limits, the payer must reconnect back to the online system before they can continue with further transactions.[17] • **Staged offline** is where after a payer has sent value to a payee, that value cannot be spent again until the payee who received that value connects back online. Some solutions can operate in all of these modes, but most were positioned as operating in an intermittently offline mode. This was suggested by solution vendors to balance usability and risk. Some noted that there were also eventual physical limitations, such as the memory size of devices storing the offline CBDC. The design choices in Chapter 3 can apply to any of these modes.

A central bank's requirements and objectives would influence their choices across these criteria. For example, a staged approach to offline transactions may suit a central bank with a limited risk appetite but may be less effective for use cases that require an extended period of time spent offline. More detailed design choices, many of which are related to these criteria, are discussed in Chapter 3. The different choices that central banks may make based on their objectives are discussed in Chapter 4.

[17] For example, after a set number of transactions sent or received, or a set amount of time spent offline.

2.2.2 Common solution vendor challenges

All solution vendors need to be able to demonstrate they are able to **meet central bank requirements**. This could include security, production readiness, operational sovereignty and compliance with existing risk frameworks. Central banks are unlikely to contract with a vendor without assurance on these key aspects, regardless of the value they offer. This could apply to all parts of a CBDC solution, but the increased risks of offline payments with CBDC add to the assurance central banks may require.[18]

Production readiness may be easier to prove for solution vendors using established technologies and standards. For example, smart cards following the EMVCo standard have been operating at scale in the market for decades and have been incrementally adding further layers of protection.[19] Solution vendors using new or emerging technologies will need to demonstrate the maturity and security of their solutions in a clear, repeatable and industry-recognised way. In some cases, no industry approach currently exists and one may need to be developed.

The central banking community has an active role to play in defining the requirements and standards that solution vendors and their technology should be assessed against. In traditional payments, standards such as ISO 20022 have shown the value of such a collaborative industry-wide approach and something similar may be valuable in the CBDC space.[20] The time spent developing established technology and the associated standards highlight the challenge involved in developing new standards.

Solution vendors should consider how they could undertake collaborations with central banks to better understand central bank requirements. Solution vendors cannot do this in isolation. Central banks should also explore how best to work with solution vendors to ensure solutions can meet central bank needs. Box A contains some examples of existing central bank work on offline payments with CBDC.

Solution vendors require **ongoing investment** to continue to develop their solutions. Nearly all solution vendors were clear in their desire for more guidance from central banks. They want to understand the problems that central banks are trying to solve and their requirements for offline payments with CBDC. This would allow solution vendors to demonstrate the business case for their solutions more clearly and help them raise further funding for their work. Ongoing funding helps vendors to make their prototypes and pilots more production-ready or allows for the development of new and novel technologies that better meet central bank requirements.

The current risk appears to be that, instead of guiding solution vendors by setting out their requirements, central banks are asking to see what exists today. In some circumstances, this may not fully meet the central bank's needs. Further, a false sense

---

[18] For example, offline payments cannot benefit from real-time risk monitoring and analysis in the same way as a connected payment. For further examples, see Chapter 5 of BIS Innovation Hub (2023a). Some vendors argued that offline payments could be considered less risky than online payments, given that an offline payment has a much smaller attack surface than an online one.

[19] See EMVCo (2022), which covers the tamper-resistant features of chips used in EMV payment cards.

[20] For an example of the value of the ISO 20022 standard, see CPMI (2022). Such work can provide an option to create a sustainable approach to innovation that learns from and avoids mistakes from the past.

of readiness can be generated if demonstrations of prototypes are misunderstood or misrepresented. This could mean that central banks do not understand the full extent of the work that could be required to make a solution secure and production ready.

If solution vendors cannot demonstrate where the future demand for their solutions will come from, it may be difficult for them to secure investment to enhance existing solutions or develop new ones. Central banks should understand the revenue models of solution vendors and consider how that fits with their own CBDC operating model and their vendor and third-party risk management frameworks. If these models are incompatible, both sides need to communicate to try to reach a workable outcome.

Box A: Examples of ongoing central bank work on offline CBDC

A number of central banks are undertaking research projects, prototypes or pilots on offline payments with CBDC. Some examples are given below. This is not intended to cover all ongoing work, but instead to highlight the variety of work ongoing and the value that this is adding to our collective understanding.

Several projects have explored the risks and trade-offs associated with offline payments with CBDC. Sveriges Riksbank's e-Krona project demonstrated consecutive offline payments but highlighted a number of potential risks.[21] Similarly, the digital euro's prototype of offline payments with CBDC discovered potential risks requiring further work.[22] The Bank of England's call for supplier interest in October 2022 to undertake an offline proof of concept noted similar challenges.[23]

A number of central banks have approached the problem of offline payments with CBDC through collaboration with telecom and mobile phone manufacturers. As SIM cards and mobile phones are potential offline payment devices, such collaborations could be particularly valuable. The People's Bank of China has added a feature to its digital yuan payment app so that mobile phone SIMs can still be used to make payments, even if they lack connectivity or power.[24] The Bank of Korea announced a collaboration with Samsung Electronics, focused on offline payments with CBDC.[25]

Many central banks note the importance of offline payments with CBDC to their ongoing work. The Reserve Bank of Australia explored P2B offline payments as part of its CBDC research project, noting the potential value of CBDC providing a digital version of a cash-like transfer.[26] The Reserve Bank of India confirmed that it is exploring offline functionality in collaboration with the private sector.[27]

---

21 See Sveriges Riksbank (2022a).

22 See European Central Bank (2023).

23 See Gov.UK Digital Marketplace (2022).

24 See Du Chuan (2023).

25 See Im Eun-byel (2023).

26 See Reserve Bank of Australia (2023).

27 See R Singh (2023).

3. Design choices for offline payment solutions

The deep-dive workshops identified a number of design choices which represent what needs to be considered when creating an offline payment solution. Some design choices limit others. For example, a high level of privacy could affect how suspicious actions in the system are detected and countered. Central banks need to consider which choices are most important to them, accepting that there may be trade-offs.

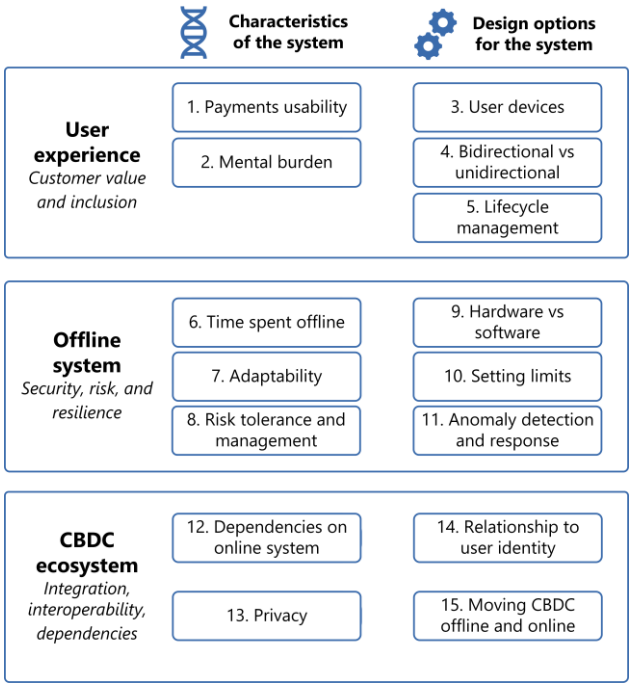
A distinction can be drawn between primary and secondary design choices.

Primary design choices are a direct consequence of a central bank's core objectives for offline payments with CBDC and there are many interlinkages across them. They should be considered first as part of the design process.

Secondary design choices remain critical when forming a holistic view of a CBDC architecture with offline payment capabilities but are less affected by a central bank's objectives. This is because they either remain the same regardless of the central bank's objective, such as the need for an exception management strategy, or they are derived from primary design choices, such as the value form of CBDC. This means that they can be considered after the primary design choices have been worked through.

3.1 Primary design choices

Primary design choices — Graph 6



A number of themes, overlaps and dependencies across choices link between these categorisations. For example, security is core and central to the offline system category but is relevant across many other choices.

The primary design choices are summarised in Graph 6. They are categorised based on whether they relate to the user experience, the offline system or the CBDC ecosystem. There remain overlaps and dependencies that cut across these categorisations. For example, taking a hardware- or software-based approach to security impacts your choice of user devices. Central banks need to consider all of their design choices as a whole, understanding overlaps and any potential trade-offs. These categories build on the logical architecture for offline payment solutions shown within the offline handbook.[28] They highlight the design choices a central bank would need to make when elaborating an offline payment solution architecture and design.

Some design choices are **characteristics of the system**, which determine how the system is set up and how it behaves. The other design choices represent discrete **design options for the system**. These concepts are discussed further in Chapter 4 and shown in Graph 10. A central bank will have requirements for the characteristics of its offline payment solution and choose design options based on these. The interconnected nature of design choices means in some instances the central bank may face trade-offs. These could be managed through an iterative design process.[29] The following provides a summary of the important aspects of each design choice. Considerations for central banks are highlighted below each choice.

3.1.1 User experience: customer value and inclusion

Central banks can meet their objectives for offline payments with CBDC only if users are able and willing to make use of their offline payment solution. This is important in jurisdictions where users already have a variety of existing solutions to choose from and for individuals or jurisdictions who are underserved by current options.

1. **Payment usability:** Users want payments to be simple, easy, quick and convenient to make. They expect that each payment should consistently take the same amount of time to make. Users must make an effort to understand new payment methods and may be reluctant to adopt one that is new or unfamiliar. They are likely to compare their experiences across different payment methods.

Central banks should ensure transaction times and the steps to make payments are consistent for users and are comparable to the user experience of existing payments.

2. **Mental burden:** Offline CBDC could introduce complexity for end users, who may not understand the need to move funds onto their device to ensure that CBDC is available to use when offline. This may differ from their experience with other forms of payment such as debit cards. Some users may struggle with the digital literacy required to operate certain devices and have specific accessibility needs.

Central banks should consider how they communicate offline CBDC to users and how their solution supports users in seamlessly managing online and offline balances.

---

28 See Chapter 4 of BIS Innovation Hub (2023a).

29 On the importance of an iterative approach in CBDC design, see Soderberg et al (2023)

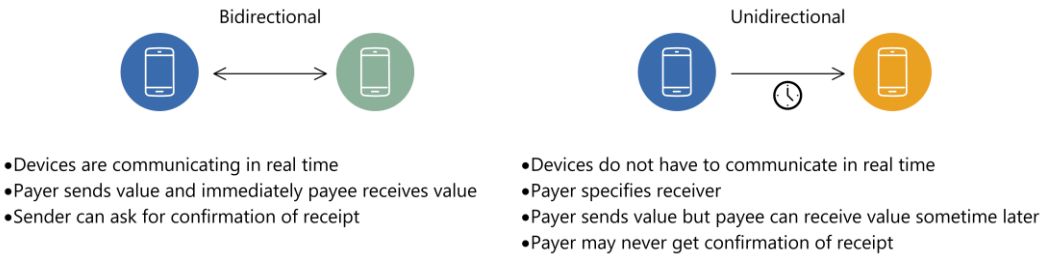
3. User devices: The most common user devices are payment cards and smartphones. There are a number of other options including custom devices, wearables, feature phones, SIM cards and key fobs. Different user devices have different costs and characteristics resulting in different potential market penetration in a given jurisdiction. Where there are several different CBDC user devices, it will be important they can interoperate, such as the ability to exchange value between a smartphone and a payment card. User devices that make use of widely accessible and interoperable technology could support increased inclusion and acceptance.

Central banks should consider which user devices best serve their users, noting that this may require multiple user devices and that different user devices should interoperate.

4. Bidirectional vs unidirectional: A bidirectional transfer involves two payment devices actively communicating to complete a transaction, with the payer's device waiting for a proof of receipt from the payee's device. A unidirectional transfer involves a payer's device specifying a payee's device and using some mechanism to send the payment from the payer to the payee. From the perspective of the payer's device, that payment has now been completed. That is true even if the payee's device does not accept the payment for some extended period of time, or if it never accepts the payment. Unidirectional transfers have the potential to support additional use cases, such as offline transfers occurring with a large distance between users who are not in direct communication. That said, unidirectional transfers, and the funds sent, stand a greater chance of getting lost. Graph 7 shows a comparison of these transfers.

Central banks should choose to have bidirectional, unidirectional or both transfer types.

Bidirectional vs unidirectional transfers — Graph 7



5. Lifecycle management: A central bank's chosen set of user devices will need to be produced, distributed to the correct end users and used for payments. They will also need to be replaced, updated, maintained or retired over time while ensuring that trust and security is guaranteed throughout.[30] This creates a requirement for a long-term operational and change management capability for the day-to-day running of any offline payment solution.

Central banks should consider the requirements for the operational capability to manage the distribution of end user devices and the maintenance of their security.

[30] See eg GlobalPlatform (2018) for an example. See also Chapter 4 of BIS Innovation Hub (2023a).

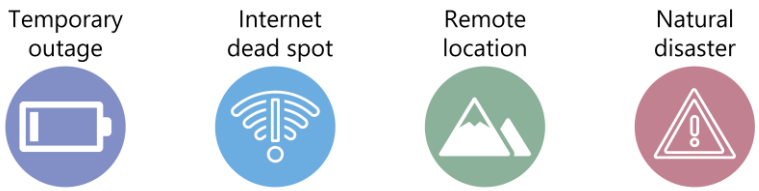
3.1.2 Offline system: security, risk and the impact on resilience

Offline systems carry additional risks compared with online systems, given that transactions are conducted outside the scrutiny of the wider system. The offline system must be designed to detect and prevent malicious behaviour, in line with a central bank's risk appetite. This is a highly complex and challenging area. The BISIH has published a security and resilience framework for CBDC systems that could be applied in the offline context.[31] Security and risk management can affect usability and the use cases that a solution supports, given that most measures rely on reconnecting to the online system after some period of time or after a set number of transactions.

6. Time spent offline: The amount of time a user can spend offline will determine the use cases the solution can support. This proceeds from the security and risk management decisions taken in the system. In general, a greater time spent offline is likely to increase the potential risk to the system. Some solutions may work poorly if offline for an extended period of time. Sample use cases are shown in Graph 8, although in reality different outages could be longer, shorter or intermittent.

Central banks should ensure their offline payment solution supports their use cases and balance this alongside their risk and security profile.

Time spent offline for different use cases — Graph 8



Different offline use cases will lead to a different requirement for time spent offline. This could be anywhere from a few minutes all the way through to several weeks or months

7. Adaptability: The desired use cases, risk tolerance and security approach may change over time. This requires that security measures can be updated, including cryptographic agility; the ability to update any cryptographic primitive used within the solution. A way to apply changes is needed when the offline device is connected to the online system, but also when the device cannot easily reconnect. This is likely to be challenging. For example, in the case of a natural disaster, there may be a need to alter limits to allow users to spend a longer period of time offline. At the same time, rolling out such changes during a natural disaster would require a way of transmitting them while lacking connectivity. This is closely related to lifecycle management.

Central banks should ensure they are able to update limits and other security measures within offline devices, balancing ease of rollout with security considerations.

[31] See BIS Innovation Hub (2023c).

8. Risk tolerance and management: Different central banks will have a different risk tolerance for their offline solution. This could be similar to what exists for banknotes today, such as considering acceptable levels of loss, counterfeiting and fraud.[32] This is linked to security, configuration of limits, and the detection of and response to anomalies in the system. This will change over time, taking into account the growth and maturity of the solution and the potential for new threats to emerge.

Central banks should consider their risk tolerance for offline payment solutions.

9. Hardware vs software-based security: Hardware-based secure elements are found in payment cards, some SIM cards and some mobile phones. They are relatively mature and provide strong protection against a variety of potential attacks.[33] Software-based protection exists, but it is less mature and generally offers less guaranteed tamper-resistance. This may mean software-based solutions are better suited to staged offline payments or use cases requiring only a few consecutive offline payments. A software-only approach may be cheaper and easier to distribute than a hardware-based approach and may offer sufficient security depending on a central bank's risk appetite. If a vulnerability is detected, a software-only approach may be easier to update than a hardware-based approach, which may require device replacement. An emerging hardware-based approach is a physical unclonable function (PUF).[34] This leverages natural randomness in the manufacture of a device to generate authentication credentials based on the device's random uniqueness. The approach is not as mature as secure elements but is an area of active exploration.[35]

Central banks should choose a security approach that matches their risk management profile while also considering their requirements for rollout and costs.

10. Setting limits: Solution vendors typically support a variety of transaction limits. The most common limits suggested are cumulative transactions, transaction values, offline holdings and expiration dates. As limits can impact the use cases that can be supported, they should be configured with use cases and risk tolerance in mind. Central banks will want to update limits over time but other actors in the ecosystem should not be able to alter or exceed the limits set by the central bank.

Central banks should set limits considering both their risk management profile and the use cases they want their offline payment solution to support.

11. Anomaly detection and response: Regardless of the security approach, an offline payment solution should be designed on the assumption it could be compromised. A CBDC system may face numerous cyber threats.[36] To ensure and maintain trust, the system needs to be able to detect anomalous behaviour and

---

32 See Chapter 5 of BIS Innovation Hub (2023a). Determining acceptable levels of risk in an offline payment solution is an important exercise for any central bank and could have a bearing on other design choices.

33 TEEs are another form of hardware-based security which typically offer more functionality but a lower level of tamper-resistance than SEs. See Chapter 4 in BIS Innovation Hub (2023a).

34 See Gao et al (2020).

35 See eg Calhoun et al (2019).

36 See BIS Innovation Hub (2023c).

provide options for responding to malicious actors. For example, this could involve blocking suspicious devices from making further payments. Such block lists would need to be circulated among offline devices, meaning there may be a lag between detection and prevention, given that offline devices would receive an updated block list only when they connect to the online system. Block lists may become lengthy over time, making them difficult to store on some user devices. Other ways are needed to isolate and manage malicious offline devices. Detection is difficult to do while a device is offline, as checks for consistency and integrity typically take place against the online ledger. This is what creates the requirement for offline devices to regularly connect to the online system. The requirement to force users to connect periodically interrupts the ability to make continuous offline payments and affects payment usability.

Central banks should ensure their solution can adequately detect and respond to malicious actors while balancing objectives around usability.

3.1.3 CBDC ecosystem: Integration and dependencies

An offline payment solution will not exist in isolation. It will need to integrate and interoperate with other payment solutions. It will have dependencies on the online system to operate, such as how and where identity is linked and stored and the movement of funds from the online system onto an offline device and vice versa.

12. Dependencies on online system: An operational offline payment solution requires a parallel operational online solution.[37] Almost all solutions are subject to a number of dependencies on the wider payment ecosystem. This includes implementing risk management, the enforcement and renewal of limits, the loading and unloading of funds and, if required, any link between an offline device and a user's identity. Many options exist for these requirements. The product breadth of different solutions varies, as discussed in Chapter 2. Some solution vendors offer an end-to-end solution where online and offline payments work in exactly the same way. Other solution vendors offer only the offline payment aspect and suggest that this can be integrated into any online ecosystem. In either case, central banks need to think about the design of their offline solution in the context of their entire payment ecosystem.

Central banks should recognise an offline system will interact with an online system and should ensure that the overall solution design is consistent across both.

13. Privacy: Central banks could either take a common approach to privacy across the online and offline systems or offer a differentiated approach to privacy between the two systems, acknowledging that the two systems are separate.[38] The level of privacy of the offline system will have a direct impact on what actions can be taken when suspicious activity is detected. For example, if there are no links between devices and user identity, there would be no way to identify potentially malicious users even if malicious devices can be blocked in the system. The level of privacy may be influenced by other actors. For example, a smartphone acting as an offline device may

---

37 The online solution does not necessarily need to also be a CBDC system. See Grym (2020).

38 All central banks surveyed said that the level of privacy of offline payments with CBDC should be either the same as or higher than the level for online CBDC payments. See Annex A of BIS Innovation Hub (2023a).

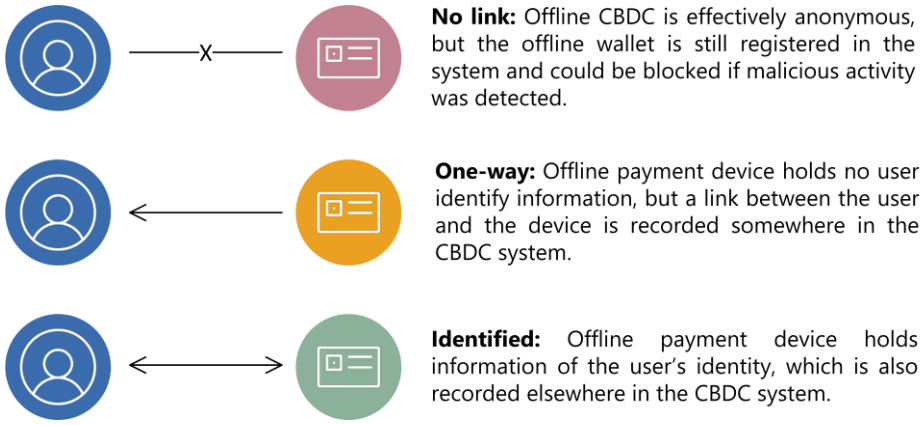
be private in the CBDC ecosystem, but its user's identity may be known by the telecom provider, which may compromise that user's privacy. This requires a balanced decision from central banks, given the multitude of potential impacts and limitations.

Central banks should consider the desired level of privacy in their CBDC system and whether or not privacy will be treated differently across the online and offline systems.

14. Relationship to user identity: Almost no solutions force offline CBDC to be linked to a specific user identity. However, the solutions do provide the ability to implement this linking, which is relevant for risk management and regulatory requirements. This will have implications for the privacy of offline CBDC payments, including the option of offering offline payments with CBDC with a high degree of anonymity. This approach could also be linked to limits. For example, allowing low-value transactions to be anonymous.[39] Some linking options are shown in Graph 9.

Central banks should determine the links between user identity, offline devices, payments and the online system and consider the implications for privacy.

Potential options for linking devices used for offline payment and user identity — Graph 9



15. Moving CBDC offline and online: A way is needed to move value onto an offline device and to move offline CBDC held on a device back online. Central banks would need to maintain a record of the sum total of offline CBDC in circulation in the same way that they monitor banknotes in circulation. There are many solutions to these requirements, but some solution vendors found these concepts challenging. This is an area where central banks may have greater understanding and could offer solution vendors additional support when communicating their requirements.

Central banks should consider how value will move from online to offline and back again and ensure they maintain a record of the sum total of offline CBDC in circulation.

[39] As noted in the privacy design choice, although the offline CBDC implementation may offer anonymity, devices for offline payments may be separately linked to a user's identity. Central banks should work with actors in the ecosystem to ensure that approaches to privacy are respected and not undermined.

3.2 Secondary design choices

Secondary design choices are still crucial in forming an overall offline payment solution design, but they can be considered subsequently to primary choices as they are less impacted by central bank objectives. They are summarised in Table 2.

Secondary design choices — Table 2

Design choice	Description
Value form of offline CBDC	How the representation of CBDC value is stored. Typical models include balances or tokens, either with a fixed value or with a variable value that can be merged and split. Depending on the solution, the value form may contain some, all, or no prior transaction history, the design of which will be determined by the risk management approach.
Transfer mechanism	How CBDC value is moved from one device to another, including both the communication method and the transfer protocol. Solution vendors demonstrated multiple communication methods including NFC, BLE, QR, strings of text and acoustic messages. The transfer protocol itself should ensure value can never be created and should minimise the scope for transactions to be torn and for value to be lost. This could include programmable use cases. For example, verifying someone's age using an offline credential before continuing an offline payment for alcohol.
Post-quantum cryptography	Offline payment solutions make use of cryptographic protocols. Quantum computers represent a threat to the security of such protocols across all financial services. Research is under way on mitigating this risk.[40] Offline payment solutions need to be able to migrate over to quantum-proof algorithms when these become widely available and robustly secured. These algorithms may have performance and compatibility effects. Equally, quantum technology could bring benefits or new solutions. This needs to be considered as part of the initial design and as an operational capability.
Exception management strategy	Incidents of lost offline CBDC cannot be avoided, whether by accident or with malicious intent. A CBDC scheme rulebook, as defined by the central bank, is needed to set out the actions to take in the event of an incident.[41] The system should provide the necessary data to implement the rulebook.
Requirements for intermediaries	Offline payments with CBDC may generate requirements for intermediaries that are additional to the requirements imposed by the online system. For example, managing offline payment incidents. CBDC holders should not at any time take any credit risk on an intermediary. This would need to be assured by either the technical design of the system or by legislation or both. Some solution vendors found this subject challenging. Some solution vendors assumed that offline intermediaries will be commercial banks. While some central banks make this design assumption, others do not.[42]

[40] See eg BIS Innovation Hub (2023b).

[41] The digital nature of offline CBDC could support functionality such as expiry dates that could allow for loss recovery. Central banks should consider the implications of this option carefully given what it might mean for the fungibility of offline CBDC and the potential for malicious actors to exploit an expiry function.

[42] See eg Bank of England and HM Treasury (2023).

3.3 Trade-offs

Some design choices inherently limit others. Table 3 below is a non-exhaustive list of some examples of the more common trade-offs. Beyond these, many links cut across multiple different aspects of design. This shows the need to design the solution holistically rather than taking each design choice in isolation.

Central banks must not compromise on any areas of design that they consider to be critical. While it is important that central banks can balance differing objectives to manage trade-offs, critical requirements must not be diluted. For example, if a given central bank has a very low risk tolerance leading to a number of core requirements around security and anomaly detection and response, if it appears that available solutions cannot sufficiently meet these requirements, then the central bank should not proceed with implementing any solution. Instead, such a central bank could collaborate with solution vendors to improve understanding and solution offerings so they can meet these critical needs.

Trade-offs Table 3

Trade-off	Description
Payment usability vs security	Users want a simple and easy payment experience. The need to regularly reconnect to the online system, because of limits, for example, could affect this. If limits are set strictly, this could reduce the scope of use cases that the offline payment solution can support. On the other hand, if there is a requirement to support weeks of offline usage, the cumulative limits required for this would be relatively large. This would introduce additional risk into the system, as the increased time between devices reconnecting online would mean greater time for malicious activities to take place beyond the scrutiny of the online system. *Central banks need to balance security, their risk appetite and for how long users need to be able to transact offline, depending on their use case.*
Cost vs security	Central banks want to ensure offline solutions are highly secure and resistant to a variety of potential attacks. However, different technologies come with different costs. This includes the costs of production, distribution, operation, management and replacement. For some jurisdictions where certain hardware is not commonly available, or where there is a large population to serve, it may be that the most secure but also most expensive solution would not be viable to roll out. In such circumstances, cheaper options, alongside other risk management practices, may be better suited to reaching a majority of the population. *Central banks need to balance the cost and security of a solution, their risk appetite and their ability to serve enough of their population.*

Risk management vs consistency	Users want a consistent payment experience. Some offline payment protocols transfer large amounts of variable transaction history with offline payments, based on their approach to risk management. As the amount of transaction history that a given payment carries will vary from transaction to transaction, this may alter the time it takes for a transaction to take place. Long transaction times could be confusing for users, who may expect each payment to take the same amount of time and have expectations based on other payment methods about the length of time a transaction should take.[43] *Central banks need to balance security and risk management with the need to offer a consistent payment experience.*
Privacy vs risk tolerance	Cash-like features for CBDC are one of several objectives for some central banks.[44] Offline payments capabilities could offer such features. For example, the ability to make low-value in-person payments with a high degree of anonymity. However, offline payments present additional risks as they happen away from any monitoring carried out by an online system and could be exploited by malicious actors, for example in money laundering activities. When considering combatting such actions, and the actors who perpetrate them, one option could be to link identity data to offline devices or offline payment data, but at the same time, such an approach could undermine any privacy objectives. Transaction limits could be another option, but these could have an impact on payment usability and user experience. Legislative requirements may be introduced in some jurisdictions that could affect how private or anonymous a central bank could make their offline payments capabilities. *Central banks need to balance the requirements for highly private or anonymous payments against the risks associated with such payments.*

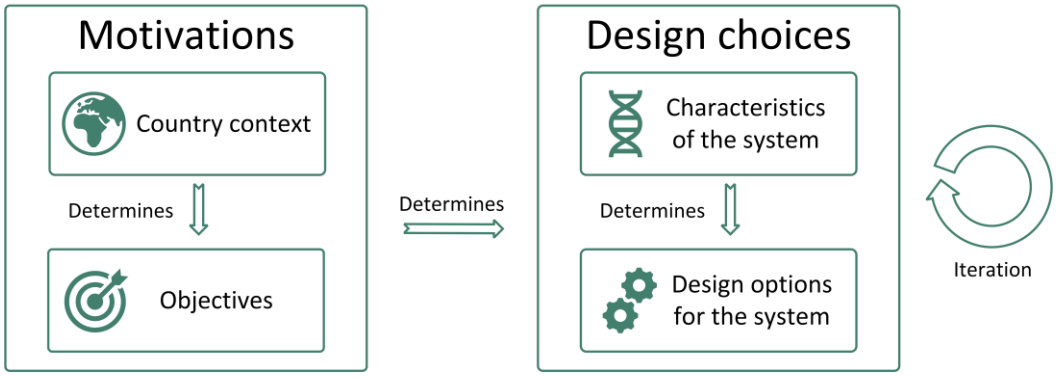
[43] Consumers may compare this with a cash payment experience, which is instant, or other digital payment methods such as contactless payments, which are near instant from the consumer perspective.

[44] See eg European Central Bank (2022).

4. Applying the design choices

Central banks must understand their motivations for offline payments with CBDC before considering the design choices. These motivations depend on their jurisdiction's context and objectives. Central banks are likely to face trade-offs when applying their motivations to different design choices. This will require an iterative design process that includes considering alternative choices or prioritisation of objectives. Graph 10 outlines the sequence of steps for this process.

The sequence of steps for applying the design choices — Graph 10



4.1 Motivations

A central bank's motivation for offline payments with CBDC is based on its context and objectives as shown in Graph 10. Table 4 shows some factors that determine a jurisdiction's context. This context determines a central bank's objectives for offline payments with CBDC. Several common objectives are discussed in Chapter 2.

Factors that influence a jurisdiction's context — Table 4

Factor	Description
Geography and demography	This might include size, population, cultural conventions and behaviours, features such as islands or mountains and risks of disruption from weather events or natural disasters.
Income	This could include per capita income, the gini coefficient and different income percentiles. This could be expanded to other indicators of wealth.
Inclusion	This includes financial, social and digital inclusion. This could include measures of digital literacy, the percentage of the population who are unbanked, or measures of the affordability of devices such as smartphones.

Payment market maturity	This might include how mature and resilient the options for making payments are, how digitised payment services are and how many different choices there are when making a payment. It could also include cash usage.
Internet and mobile network coverage	This might include whether there is a difference in coverage in different areas and how reliable and resilient the service is. For example, between urban and rural. It could be expanded to consider smartphone penetration.

4.2 Design options and characteristics of the system

The design choices are outlined in Chapter 3 and summarised in Graph 6. Some design choices are **characteristics of the system**, and how it behaves. The others represent discrete **design options for the system**.

The desired characteristics of the system are based on a central bank's motivations and create a set of requirements. These requirements determine the design options for the system. This creates a relationship between the desired characteristics of the system and the design options that a central bank chooses. For example, if a central bank has the desired system characteristic of a high level of privacy, this will determine the design options around the relationship to user identity.

Some use cases may create a set of desired characteristics and design options that are incompatible. For example, if a central bank has the desired characteristics of users spending a long period of time offline, but also has a low risk tolerance, then it may be difficult to set limits to satisfy both of these characteristics and achieve a central bank's underlying use case. This is where an iterative design process could be valuable, considering different options, including the priority of different desired characteristics. Central banks should consider what design choices work best based on their motivations and consider the extent to which any trade-offs are manageable.

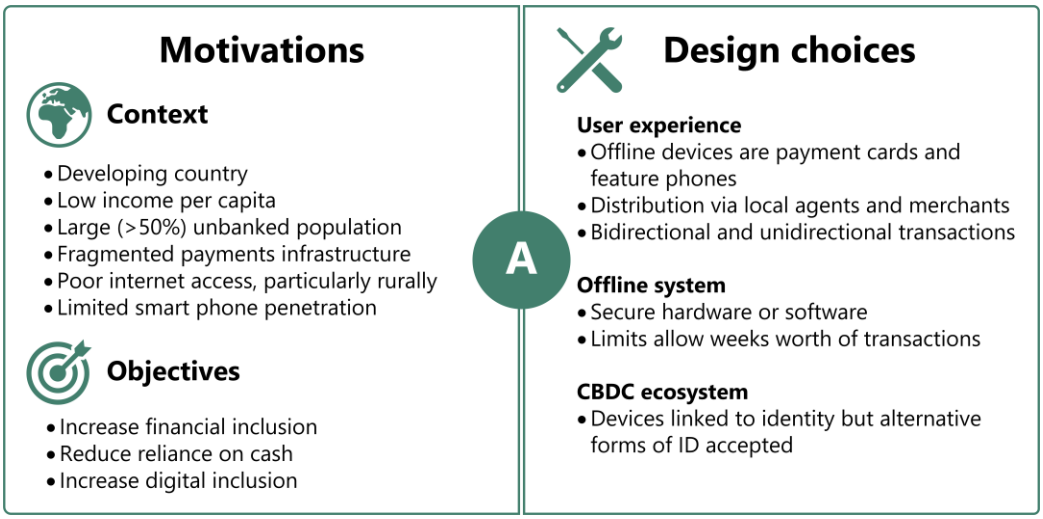
4.3 Illustrative scenarios

To demonstrate this approach, three illustrative scenarios with different motivations have been set out. These are non-exhaustive but **demonstrate how a central bank could apply this approach in its own context**. A detailed breakdown and comparison of each can be found within Annex A. The scenarios are as follows:

- **Jurisdiction A** is a developing country with a large unbanked population and a fragmented payments infrastructure.
- **Jurisdiction B** is a multi-island nation with higher risks of natural disaster and weather events that lead to regular disruption.
- **Jurisdiction C** is an advanced economy with mature payments and internet infrastructure but with declining transactional cash usage and acceptance.

4.3.1 Jurisdiction A: Growing inclusion and infrastructure

Jurisdiction A: Growing inclusion and infrastructure Graph 11



Motivations: Jurisdiction A is a developing country with low income per capita and a large unbanked population. Payments and internet infrastructure is fragmented with limited internet access or connectivity, particularly in rural areas.

Their primary objective is to increase financial inclusion in the population by helping the unbanked gain access to financial services. There may be additional benefits from beginning to build out a more formalised financial infrastructure. This may reduce the reliance on cash and the associated costs of distribution. It may also mean that a larger percentage of the population is making use of digital services.

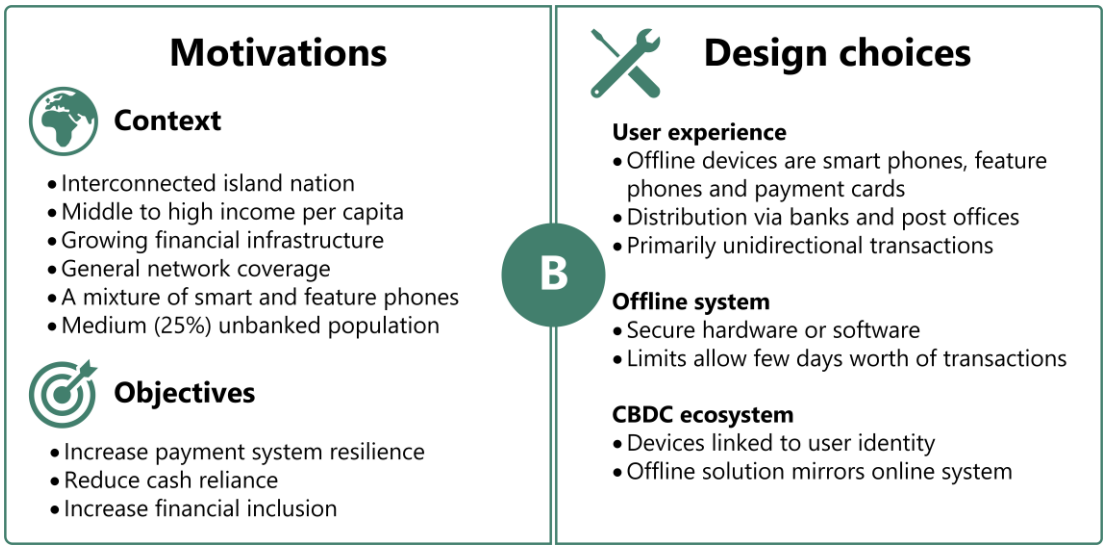
Design choices: Users make use of payment cards and feature phones, which can be purchased from local agents and merchants, and are widely available even in remote rural areas.

Device security can be hardware- or software-based depending on which is more available, appropriate, cheaper and easier to rollout. Limits are set to support infrequent online connections, given limited internet access. For example, these limits could allow an average household to undertake a weeks' worth of transactions before needing to connect back online. This may also save user costs associated with connecting to networks, which could support adoption amongst poor communities.

Payment devices would be linked to user identity, but alternative forms of ID would be accepted to help the unbanked be able to participate in the CBDC ecosystem. This would also increase unbanked users' integration into the financial services ecosystem. The system would be likely to take a mixed approach to managing suspicious activity, as the linking of user identity to payment devices would be different for different users. Block lists could be one solution for this but may be challenging to circulate given the intermittent connectivity. Other options would require exploration. Any follow-up actions would be dependent on the amount of KYC undertaken on that specific user, and the desired approach to suspicious activity within the jurisdiction.

4.3.2 Jurisdiction B: Increasing resilience within complex geographies

Jurisdiction B: Increasing resilience within complex geographies Graph 12



Motivations: Jurisdiction B is a multi-island nation. Due to this geography it is at an increased risk of natural disasters or weather events that lead to outages and communication issues. Some of the population remains unbanked and this varies by location in the jurisdiction. Income per capita, financial infrastructure and network coverage are all growing and improving.

The primary objective is to increase payment system resilience to take the unique geography into consideration, as well as the potential for periodic outages. Additional benefits may be found in increasing financial inclusion and making this uniform across different islands and reducing the reliance on cash, which is expensive to move between islands.

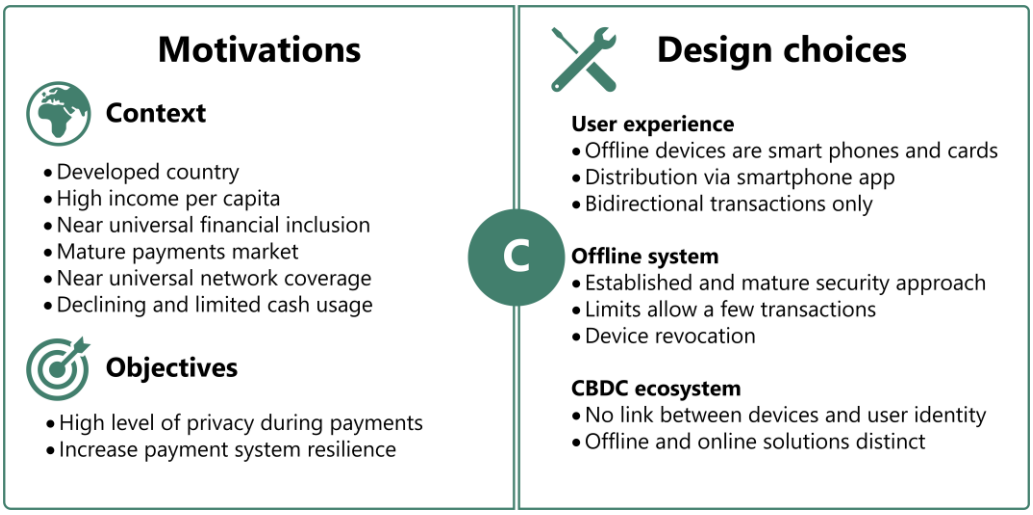
Design choices: Users can sign up for smartphones, feature phones and payment cards at a trusted intermediary such as a commercial bank, post office or mobile network operator. This would provide trust and security in the system. Unidirectional transactions would be a valuable feature to add further resilience, given that outages are unpredictable.

Device security can be hardware- or software-based, depending on the user device. Limits are set to allow spending over common outage lengths, for example, allowing a few days' worth of transactions. Limits may also differ for different user devices and based on how much identity data a user has provided.

Devices would be linked to a user's identity as part of the onboarding process. This would give the jurisdiction a number of options in terms of detecting and responding to malicious activity. They could make use of device block lists or seek to identify specific users who have undertaken malicious actions. This would need to be balanced with the approach taken to privacy within the system.

4.3.3 Jurisdiction C: Maintaining privacy as physical cash usage declines

Jurisdiction C: Maintaining privacy as cash usage declines Graph 13



Motivations: A developed nation with a high income per capita, near universal financial inclusion, mature payments infrastructure, near universal network coverage and high smartphone penetration. There is declining and limited transactional use of cash with some merchants no longer accepting it.

With cash on the decline, the primary objectives are to maintain a privacy or anonymity-preserving form of payment and in providing additional payment system resilience from another payment option in the event of disruption.

Design choices: Users sign up for the service via a smartphone app. This leverages existing digital and financial infrastructures. It would support bidirectional payments only, to mirror a cash-like exchange. There may be a need for alternative user devices such as cards or bespoke devices to support certain users and communities.

Given the risks around highly private or anonymous payments, device security must be based on established and mature technologies. Initially, devices may require a secure element and use hardware-based security. However, any security approach that can prove it meets the security requirements of a central bank would be viable. This could include software-based approaches, or the use of PUFs. Options may grow over time as more devices and approaches meet the security requirements.

The risks associated with highly private or anonymous payments could potentially mean that limits would be set with rigour, for example, by allowing only a few transactions at a time before a user needs to connect back online. Limits may also seek to comply with existing AML, CFT and KYC regulations. Alternatively, legislation may need to be updated for CBDC, to align with the central bank's objectives. Without some link between user identity and devices, suspicious activity could be dealt with via device revocation, however the practicalities would need to be better understood. The offline payment solution is likely to be distinct from the online solution, reflecting the focus on a cash-like use case.

5. Conclusion

This guide has shown how central banks can map their objectives for offline payments with CBDC onto the design choices necessary to implement an offline payment solution. It has built on the BISIH's handbook for offline payments with CBDC by focusing further on solution design and requirements to support central banks when moving from an understanding phase into a design phase.

The main takeaways for central banks are highlighted below:

Offline payments with CBDC are complex and may require some acceptable trade-offs as part of their design. This guide has highlighted a number of design choices that would need to be considered for an offline payment solution. These choices do not always complement each other. Central banks should be clear on which design choices are most important to them when designing their solutions.

Central banks should understand their context and objectives for providing offline payments with CBDC before applying any design choices. This process will ensure that a central bank designs, procures and implements a suitable offline payment solution. Different central banks will have different objectives for offline payments with CBDC, leading to different requirements. Their chosen solutions should be designed to meet their specific context, objectives and related requirements.

Design choices must be approached holistically and not in isolation. For example, the solution must provide the appropriate user experience, while managing the central bank's risk appetite. In turn, risk and security must be considered alongside the desired approach to privacy and identity linking across users, their devices, and the online system. Some of the core links between objectives, characteristics and design options for the system are shown in Graph 1. There will be further relevant links beyond those shown.

An iterative approach to design should be taken to work through various potential options and explore ways to overcome trade-offs. An iterative approach would allow central banks to explore alternative options and find the set of design choices that best meets their needs.

Central bank requirements should determine the offline payment solution. The current risk is that, instead of guiding solution vendors with their requirements, central banks are just asking to see what exists today. This may not meet central bank needs and does not help solution vendors understand how they could develop their solutions. A requirement-first approach ensures that solutions are fit for purpose and gives solution vendors greater guidance.

Central banks should be a driving force for collaboration and innovation for offline payments with CBDC. This will support solution vendors in developing new technologies, or in improving and launching existing prototypes and pilots. Central banks are uniquely positioned to drive this forward but cannot be complacent and expect solution vendors and the private sector to do this on their own.

References

Bank for International Settlements, 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 (2021): *Central bank digital currencies: executive summary,* September.

Bank of England and HM Treasury (2023): *The digital pound: a new form of money for households and businesses?,* February.

BIS Innovation Hub (2023a): *Project Polaris: a handbook for offline payments with CBDC,* May.

——— (2023b): *Project Leap: Quantum-proofing the financial system*. June.

——— (2023c): *Project Polaris Part 2: A security and resilience framework for CBDC systems,* July.

CPMI (2022): *Harmonisation of ISO 20022: partnering with industry for faster, cheaper, and more transparent cross-border payments,* September.

Calhoun, J, C Minwalla, C Helmich, F Saqid, W Che and J Plusquellic (2019): "Physical Unclonable Function (PUF)-Based e-Cash Transaction Protocol (PUF-Cash)", *Cryptography.3.18.10.3390,* July.

Du, Chuan (2023): "E-yuan app adds payment function for when mobiles are offline, out of power", Yicai Global, January, www.yicaiglobal.com/news/e-yuan-app-adds-payment-function-for-when-mobiles-are-offline-out-of-power.

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

European Central Bank (2022): *Progress on the investigation phase of a digital euro,* September.

——— (2023): *Digital euro – Prototype summary and lessons learned,* May.

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

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

Gov.UK Digital Marketplace (2022): "Central Bank Digital Currency (CBDC) Proof of Concept and Research Offline payments", October, www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/18203.

Gyrm, Aleksi (2020): "Lessons learned from the world's first CBDC", *BoF Economics Review,* No. 8.

Hayashi, F and S Minhas (2018): "Who are the unbanked? Characteristics beyond income." *The Federal Reserve Bank of Kansas City Economic Review, Second Quarter*, June.

Im, Eun-byel (2023): "BOK, Samsung join hands for offline payment using CBDC", *The Korean Herald*, May, www.koreaherald.com/view.php?ud=20230515000719.

Kosse, A and I Mattei (2023): "Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto", *BIS Papers*, no 136, July.

Minwalla, C, J Miedema, S Hernandez and A Sutton-Lalani (2023): "A central bank digital currency for offline payments", *Bank of Canada Staff Analytical Note*, no 2023-2, February.

Reserve Bank of Australia (2023): *Australian CBDC Pilot for Digital Finance Innovation: Project Report,* August.

Singh, R (2023): "Looking at offline functionality of central bank digital currency: RBI's Executive Director", CNBC-TV18, March, www.cnbctv18.com/finance/cbdc-digital-rupee-looking-at-offline-functionality-of-central-bank-currency-rbi-executive-director-16090091.htm.

Soderberg, G, J Kiff, H Tourpe, M Bechara, S Forte, K Kao, A Lannquist, T Sun and A Yoshinaga (202): "How should central banks explore central bank digital currency? A dynamic decision-making framework", *IMF Fintech Notes*, no 2023/008, September.

Sveriges Riksbank (2022a): *E-krona pilot phase 2,* April.

——— (2022b): "Offline payments can improve resilience to disruption", *Payments Report 2022*, December.

Annex A: Example jurisdiction comparison

The tables below summarise various aspects of the example jurisdictions discussed in Chapter 4. Table A.1 compares the different context and objectives. Table A.2 then compares the different suggested solutions. Table A.3 considers how potential variations in a jurisdiction's context affects its objectives, and how this impacts the design choices. This shows that jurisdictions may pursue similar solutions, but there is likely to still be some differences based on specific context.

These stylised examples are offered to support central bank thinking and discussion. They should not be taken as a definitive approach to solution design.

Example jurisdiction context and objectives — Table A.1

	Jurisdiction A	**Jurisdiction B**	**Jurisdiction C**
Geography and demography	Some areas exposed to natural disasters	Interconnected islands with high risk of natural disasters	Limited exposure to natural disasters
Income	Low	Middle	High
Inclusion	Large share (>50%) of people unbanked	Medium share (25%) of people unbanked	Small share (<5%) of people unbanked
Cash usage	Regular cash usage	Regular cash usage	Declining cash usage
Payments market	Fragmented payments infrastructure	Developing payments infrastructure	Mature payments infrastructure
Internet and mobile network coverage	Limited network coverage, particularly in rural areas	General network coverage, but regular outages	Near universal network coverage
Mobile phone penetration	Limited smartphone penetration, some feature phone use	Some smartphone penetration, some feature phone use	High smartphone penetration
Primary objectives	Increase financial inclusion	Increase payment system resilience	Offer something with cash-like features for privacy reasons
Secondary objectives	Build out financial services infrastructure	Increase financial inclusion	Increase payment system resilience

Example jurisdiction solutions — Table A.2

	Jurisdiction A	Jurisdiction B	Jurisdiction C
User experience			
User devices	Payment cards and feature phones	Smartphones and payment cards	Smartphones and payment cards
Lifecycle management	Sign up and receive device via local physical touchpoint such as a merchant	Sign up and receive or register device via trusted intermediary such as a commercial bank or post office	Sign up and register device via a smartphone app
Bidirectional vs unidirectional	Could support both	Could support both. Given uncertainty of outages, unidirectional payments could be important	Mirroring a P2P cash transaction, bidirectional payments only
Offline system			
Hardware vs software	Either, dependent mostly on cost of a given user device	Either, dependent mostly on risk management	Mature established approaches that meet security requirements
Setting limits	Limits set to support infrequent connection online eg a week's worth of transactions	Limits set to allow spending over common outage period eg a few days' worth of transactions	Limits set strictly to manage risks of anonymity eg a few transactions
Detection and response	Mix of user blocking and device revocation	Suspicious users may have CBDC activity limited or blocked	Revocation of suspicious devices is strictly enforced
CBDC ecosystem			
Relationship to user identity	Link between device and identity, but large variety of accepted forms of identity to support the unbanked	Link between device and identity	No link between device and identity
Moving CBDC offline and online	Offline solution can mirror or be distinct from online system	Offline solution could mirror online system to increase usability	Offline solution distinct from online system

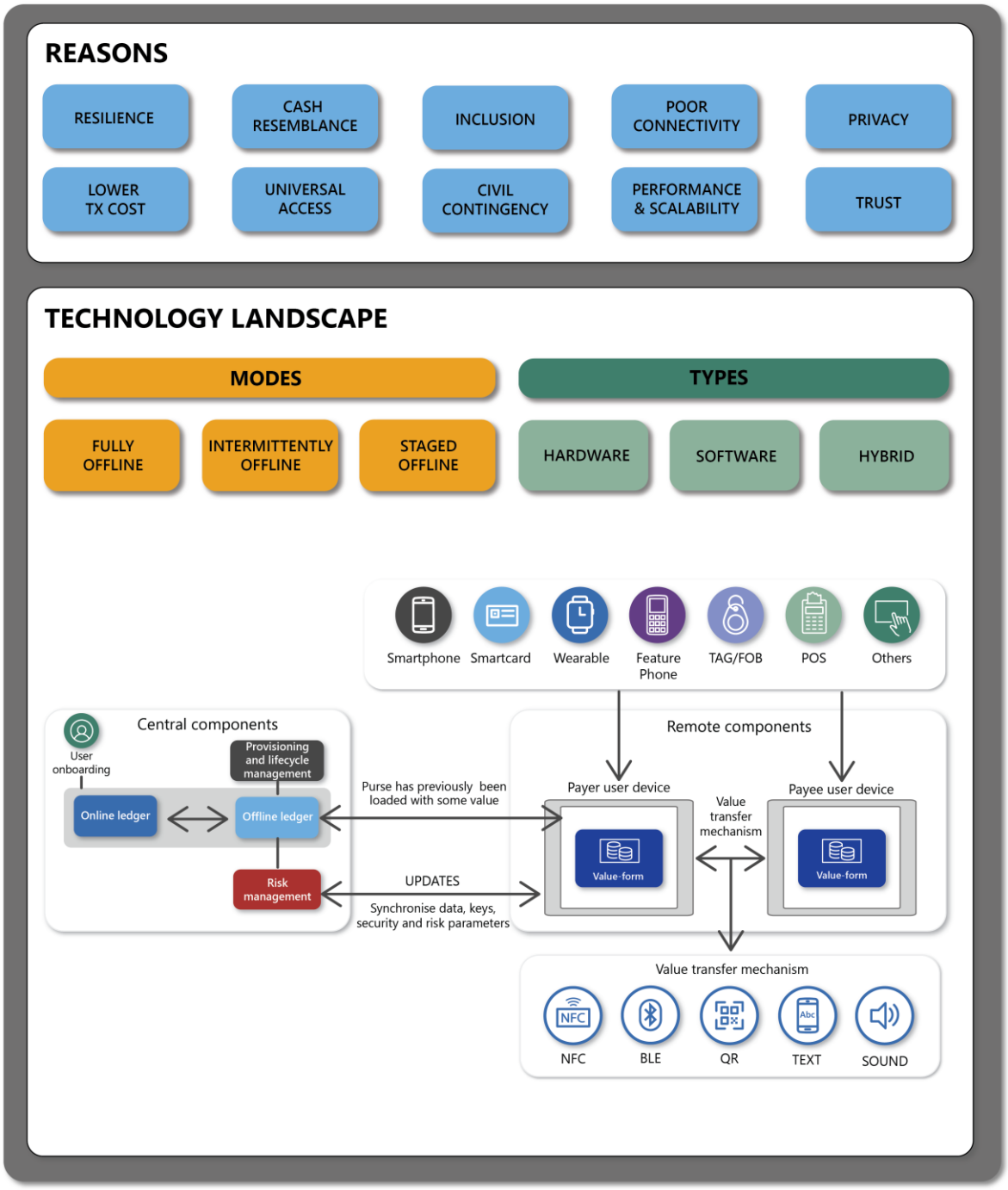
Potential variations in example country context — Table A.3

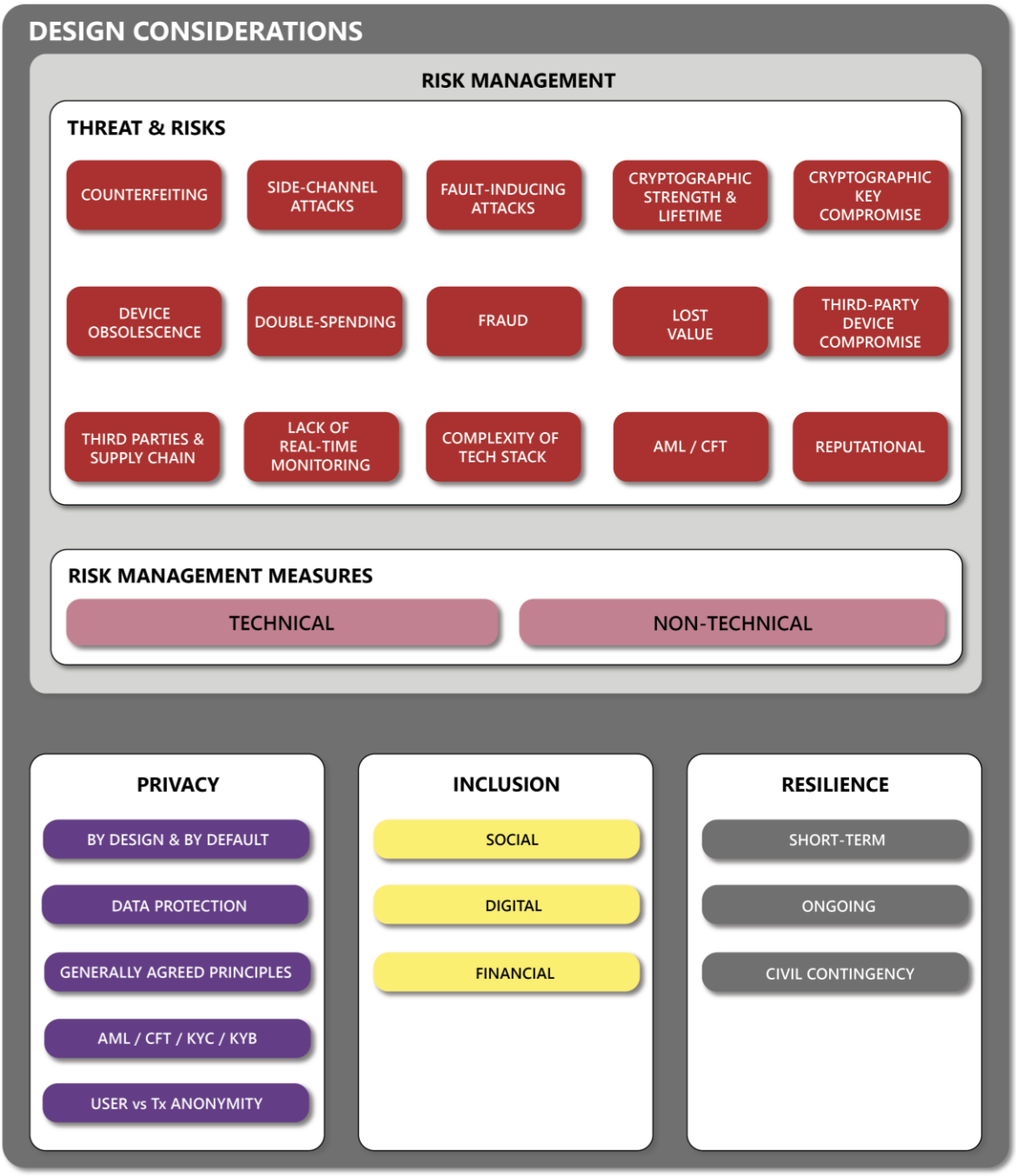
Variation in context	Impact on objectives	Impact on design choices
Jurisdiction A		
Advanced economy with remote or isolated communities that struggle with financial and digital inclusion challenges	Greater focus on universal access and bringing isolated groups to similar level of inclusion to wider population	Instead of payment cards and feature phones, may have the money to invest in a bespoke offline device Distribution of devices may be via public sector channels as it may not be a profitable service for the private sector
Large population and a significant gap between urban and rural areas in regard to financial inclusion, payment infrastructure and internet access	Building out of payment infrastructure and internet access has equal weight to improving financial inclusion	Instead of payment cards and feature phones, smartphones may be important to bridge the urban-rural gap More likely to use software-based security to manage rollout and cost across the large population
Jurisdiction B		
Jurisdiction where transactional cash usage and acceptance has declined significantly and the risk of natural disaster or civil contingency event is high	An additional objective of offering cash-like functionality to make P2P payments without connectivity	Limits likely to be broad eg to support a few weeks of transactions, given the natural disaster use case Offline solution likely to be distinct from the online solution, given that it supports a specific use case
Jurisdiction C		
Jurisdiction with a developing economy, fragmented payments infrastructure and high dependency on cash	An additional objective of reducing reliance on cash and offering a digital alternative	Instead of smartphones, may use payment cards based on cost and ease of distribution and rollout Limits likely to be broader eg to support a few days of transactions to encourage user adoption and reflective of a greater risk tolerance

Annex B: Map of offline payments with CBDC

Graph B.1 shows a full map of offline payments with CBDC, covering the full scope of the BISIH's handbook for offline payments with CBDC. This design guide provides more in-depth coverage of the technology landscape box. The design choices discussed in Chapter 3 build on the logical architecture shown below.

Map of offline payments with CBDC — Graph B.1




DESIGN CONSIDERATIONS
RISK MANAGEMENT
THREAT & RISKS
COUNTERFEITING
SIDE-CHANNEL ATTACKS
FAULT-INDUCING ATTACKS
CRYPTOGRAPHIC STRENGTH & LIFETIME
CRYPTOGRAPHIC KEY COMPROMISE
DEVICE OBSOLESCENCE
DOUBLE-SPENDING
FRAUD
LOST VALUE
THIRD-PARTY DEVICE COMPROMISE
THIRD PARTIES & SUPPLY CHAIN
LACK OF REAL-TIME MONITORING
COMPLEXITY OF TECH STACK
AML / CFT
REPUTATIONAL
RISK MANAGEMENT MEASURES
TECHNICAL
NON-TECHNICAL
PRIVACY
BY DESIGN & BY DEFAULT
DATA PROTECTION
GENERALLY AGREED PRINCIPLES
AML / CFT / KYC / KYB
USER vs Tx ANONYMITY
INCLUSION
SOCIAL
DIGITAL
FINANCIAL
RESILIENCE
SHORT-TERM
ONGOING
CIVIL CONTINGENCY

Acknowledgements

Bank for International Settlements

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

Ben Dovey (Adviser)

Björn Segendorff (Adviser)

Grímur Sigurðarson (Adviser)

Hachem Hassan (Adviser)

Sidney Lampart (Adviser)

Susanne Bohman (Adviser)

William Zhang (Adviser)

Xin Zhang (Adviser)

Consult Hyperion

Tim Richards, Principal Consultant

Neil McEvoy, Founder

Gary Munro, Technical Director

Tim Allen, Sales Director EMEA

Central bank observers for the deep-dive exercise

Johanna Schreck, Fintech Expert (Bank of Finland)

Miki Kuusinen, Adviser (Bank of Finland)

Tomer Mizrahi, Chief Technology Officer (Bank of Israel)

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

Sigríður Dís Guðjónsdóttir, Special Adviser (Central Bank of Iceland)

Barbora Kalmaityte, Market Infrastructure Specialist (European Central Bank)

Holger Hausdorf, IT Application Development Specialist (European Central Bank)

Kjetil Watne, Special Adviser Payments (Norges Bank)

Lasse Meholm, Project Manager Technology (Norges Bank)

Terje Åmås, Special Adviser Payments (Norges Bank)

Henrik Axelsson, Technology Expert (Sveriges Riksbank)

Ian Vitek, Risk Expert (Sveriges Riksbank)

Veljko Andrijasevic, Technology Expert (Sveriges Riksbank)

Solution vendor participants for the deep-dive exercise

BitMint

Crunchfish

FIS Global and M10 Networks

Giesecke+Devrient

Google

IBM

IDEMIA

SWN Global

Thales and Secretarium

ToneTag

WhisperCash

Worldline

Input and feedback

John Velissarios, Founder and Director (Otranto)

Vincent Mele, Founder and Director (Otranto)

Special acknowledgements

Cecilia Skingsley, Ross Leckow, Codruta Boar, Carmen Arias, Sonja Davidovic, Cristina Picillo, Daniel Eidan, Jack Ho, Karen Martin, Andreas Adriano, Alan Soughley.

Bank for International Settlements (BIS)

ISBN 978-92-9259-701-6