Bank of England

The digital pound: Technology Working Paper

February 2023

Bank of England

The digital pound: Technology Working Paper

February 2023

Contents

Executive summary

This paper accompanies the digital pound Consultation Paper (CP), 'The digital pound: a new form of money for households and businesses?', and outlines the Bank of England's (the Bank's) thinking on the technical requirements and design considerations for a UK central bank digital currency (CBDC).

This paper sets out the Bank's emerging thinking on CBDC technology and seeks feedback on the potential approach to important technology considerations. This paper does not set out a final design for CBDC. Rather, it sets out one possible approach to CBDC architecture. The Bank's thinking on these matters will evolve as our work accelerates. This paper and the digital pound CP are products of the 'research and exploration phase' of CBDC development, and mark the start of the 'design phase' (Figure 2).

In the design phase, the Bank will conduct experimentation which will inform an evaluation of the technology feasibility of CBDC and help to determine the optimal design and technology architecture.

This paper builds on the functional and economic design choices for CBDC, which are outlined in the digital pound CP.

The Bank and His Majesty's Treasury (HM Treasury) have identified two primary motivations for a UK CBDC: sustaining access to, and promoting the usefulness of, central bank money; and promoting innovation, choice and efficiency in domestic payments. These motivations have informed the functional and economic design choices for CBDC, which are set out in the digital pound CP.

The platform model is currently the preferred model for offering a UK CBDC (Figure 4). In this model, the Bank hosts the core ledger and an application programming interface (API) layer. The API layer would allow private sector firms, known as Payment Interface Providers (PIPs) and External Service Interface Providers (ESIPs), access to the core ledger functionality in order to provide user services. Access to the core ledger would be subject to approval by the Bank, based on objective and transparent criteria, and subject to PIPs and ESIPs having appropriate regulatory status.

This paper explores six technology design considerations, which help to organise and guide the Bank's work on CBDC technology.

The design considerations outlined in this paper are privacy, security, resilience, performance, extensibility and energy usage. These considerations guide the Bank's current thinking on the technology requirements for a UK CBDC and will likely have significant impact on the design choices for CBDC.

Privacy: The privacy design considerations are informed by the Bank and HM Treasury's public policy objectives related to privacy. The CBDC system would be designed to protect user privacy, while allowing PIPs and ESIPs the minimum necessary access to transaction data needed to provide CBDC services and to fulfil their legal and regulatory obligations. The Bank considers that privacy-enhancing technologies (PETs) might assist in meeting these requirements. However, it is important to be mindful of the complexities that PETs may introduce and the impact they might have on the other technology design considerations.

Security: It is critical that any CBDC design identifies and guards against security risks. A CBDC may be a potential target for cyber threats from a range of threat actors. The security risks could increase due to additional functionality of a CBDC, as well as the number of ecosystem participants. To manage new and existing risks, the CBDC system could be designed to support the rapid adoption of new cryptographic algorithms, use secure access management, and incorporate a comprehensive security assurance programme. The Bank might also employ a layered security approach, which involves multiple layers of security controls.

Resilience: The CBDC system should be resilient to disruption. Disruption may have far-reaching consequences for user confidence, data integrity and financial stability. Resilience might be achieved through containment and redundancy mechanisms. The Bank has established preliminary resilience requirements for a CBDC, including operating 24/7. Current RTGS and CHAPS services have a target uptime of at least 99.95%, and that would constitute a minimum expectation for Bank-managed CBDC infrastructure. However, we will also explore whether an uptime target of closer to 100% would be appropriate and deliverable (in particular 99.999%).

Performance: The CBDC system should be able to handle a high number of transactions and confirm and settle these transactions as quickly as possible. The Bank estimates that throughput of approximately 30,000 transactions per second, and confirmation and settlement in under one second, might be needed. To enable high performance, the system might utilise certain techniques, including horizontal scaling, multi-destination payments and offline payments.

Extensibility: Extensibility refers to the ability to add new functionality to a system. The CBDC system should have an extensible design, allowing PIPs and ESIPs to implement additional functionality without affecting user services. There are several factors to consider in designing an extensible CBDC system, including using a composable architecture, which focuses on defining building blocks that can be combined to achieve the required functionality of the CBDC system. The Bank might also examine the implications of using open-source components, and any vulnerabilities that may arise due to third-party dependencies.

Energy usage: The CBDC system should be energy efficient and designed in a way which minimises any impact on the environment. Therefore, Bank-managed CBDC infrastructure

would, at the very least, need to be as energy efficient as existing payment infrastructures. The Bank will evaluate the CBDC architecture for opportunities to optimise energy efficiency.

The paper sets out an illustrative conceptual model, which is based on the platform model of CBDC.

The conceptual model includes a number of different components, including the core ledger, analytics, alias service and API layer. This paper outlines how these components might operate and assesses some of the ways that ecosystem participants – the Bank, PIPs, ESIPs, and users – would interact with these components. This includes the devices and payments a CBDC might need to enable, as well as interoperability, programmability and offline payments.

Core ledger: The core ledger would provide the minimum necessary functionality for CBDC, and must meet the Bank's performance, resilience and privacy requirements, while maintaining consistency at all times. Distributed ledger technologies and blockchain-based solutions might have advantages in guaranteeing consistency and resilience, but they also present privacy, scalability and security challenges. Centrally governed, distributed database technologies might achieve the ledger requirements without such limitations. Therefore, these technologies might be appropriate for the core ledger design.

Analytics: The Bank may need to collect operational metadata for analysis of system status and performance. This would allow the Bank to maintain the core ledger and the API layer. The Bank could also collect aggregate data, subject to effective anonymisation and privacy protections, in order to undertake economic and policy analysis. These analytics would take place in a data platform, away from the core systems, and would not involve the collection or analysis of personal data.

Alias service: The alias service would manage the range of different identifiers that might be used to route transactions between users. The CBDC system might also use aliases to interoperate with existing payment infrastructures. This would allow users to choose between using well-known aliases and disposable aliases. In addition to enabling interoperability, aliases would also conceal the core wallet identifier. The initial alias design might include phone numbers, a primary account number (PAN), account number and sort code, and wallet aliases.

API layer: The API layer would allow PIPs and ESIPs to access core ledger functionality in order to offer services to users. The API layer would include an API gateway, which is an entry point for API calls, and an API service, which would implement the core functionality. There are several matters to consider in designing this, including using security controls to prevent denial of service attacks and implementing authentication or authorisation functionality in a standardised manner. API specifications might standardise data and information exchange by orchestrating CBDC payment flows.

Devices and payments: CBDC should be widely available and accepted in-store, online and peer-to-peer. Users should be able to make and receive payments using smart devices, smart cards, ecommerce websites and applications, and existing point-of-sale technologies. The Bank would need to establish standards to ensure a consistent minimum level of functionality and security. User balances would be recorded on the core ledger, but it might be necessary to store some balances locally to support offline payments. PIPs and ESIPs would carry out user authentication.

Interoperability: CBDC would be interoperable, allowing conversion between CBDC and other forms of money, particularly cash and bank deposits. Subject to further evaluation and taking account of wider developments, this might be enabled through utilising existing payment infrastructure, such as Faster Payments System, New Payments Architecture or LINK. Further integrations might be added later to support specific payment or settlement needs.

Programmability: The Bank will not pursue central bank-initiated programmable functions. This means that the Bank will not program CBDC to restrict its use. But PIPs could, with user consent, implement programmability features which are designed to give users greater functionality from their wallets and CBDC holdings. These could include automated payments or programmable wallets. The CBDC system might also enable a wide range of other programmable features, including payment-versus-payment, delivery-versus-payment and smart contract functionality, by implementing locking mechanisms, which PIPs and ESIPs can access through the API layer.

Offline payments: The CBDC system might enable offline payments. This could be useful in increasing system resilience in the event of network disruption. However, offline payments could also increase the risk of double spend, and create challenges in verifying the authenticity of funds. Additionally, offline payments could introduce complexities that affect system security and performance.

The considerations raised in this paper will be examined further in the design phase.

This paper represents our high-level approach to some of the key technology considerations and technical requirements for a UK CBDC. They will be examined further and adjusted iteratively during the next phase of our work.

The Bank is seeking feedback on the matters presented in this paper, particularly on the specific questions outlined in Section 5. This will feed into our work on CBDC and ensure that feedback and challenge from stakeholders is taken into account at an early stage of our technology work.

How to respond

Written responses to any of the questions outlined in Section 5, or any other relevant observations, are requested by 7 June 2023.

Please respond via this **survey**.

If you have any comments or enquiries, please address them to:

CBDC Unit
Bank of England
Threadneedle Street
London
EC2R 8AH

CBDC@bankofengland.co.uk

1: Introduction

This Technology Working Paper (TWP) focuses on the technical requirements and design considerations related to a digital pound. By setting out, at an early stage, a high-level approach to key technology considerations, and by proposing an illustrative technology model, the Bank aims to generate feedback and challenge that can inform our future technology work.

The **digital pound Consultation Paper** (CP) explains that although no final decision can be taken at this stage, the Bank of England (the Bank) and His Majesty's Treasury (HM Treasury) judge that a digital pound (hereafter central bank digital currency (CBDC)) is likely to be needed in the future, and the Bank and HM Treasury are proposing to accelerate work on its architecture.

The digital pound CP is consulting on the policy objectives and high-level design for a UK CBDC. It sets out why there is a likely need for a CBDC, its implications for the Bank's objectives of monetary and financial stability, the proposed public-private partnership to provide a CBDC, and the model of CBDC the Bank intends to examine further in the next stage of our work. This paper considers the technology implications of the Bank and HM Treasury's policy objectives for a UK CBDC, and the economic and functional design choices set out in the digital pound CP, using the platform model of CBDC outlined in that paper.

This paper accompanies the digital pound consultation. This paper is not a consultative document as we are not making a decision on a specific proposition. Instead, it sets out the Bank's early stage thinking on CBDC technology and seeks feedback on the potential approaches to important technology considerations. By setting out an illustrative conceptual model for a UK CBDC, which builds on the platform model, this paper offers a basis for further discussion and exploration. We invite stakeholders and technology experts to provide feedback and challenge on the matters set out in this paper, including the specific questions listed in Section 5.

Figure 1: Overview of the digital pound CP and the TWP

The Bank's thinking on the technology implications of CBDC will mature and evolve as our work develops.

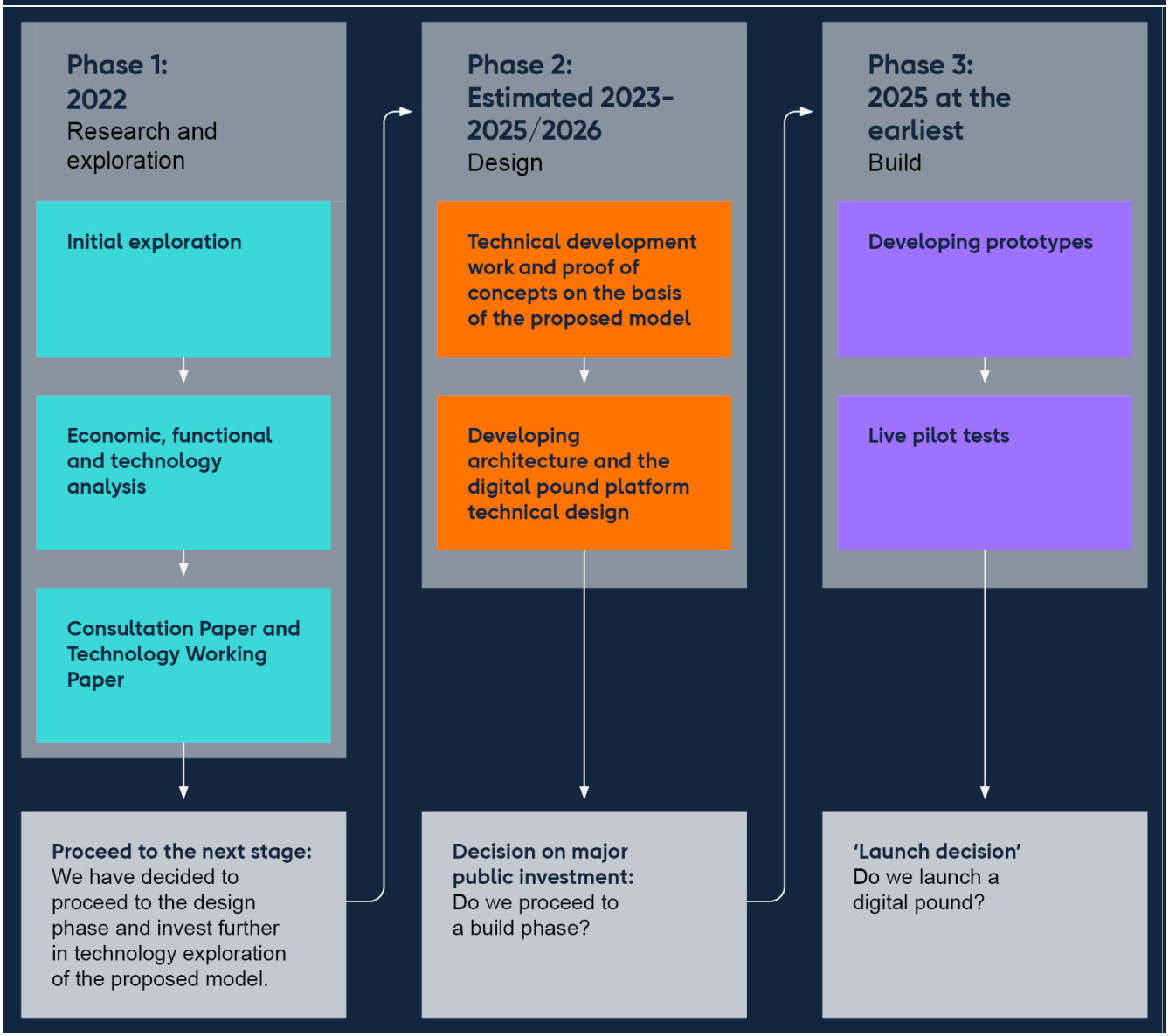
It is too early to take a decision on whether to build a UK CBDC. As such, it is not yet necessary to make firm decisions on any options for the architectural design or technology solution for a UK CBDC. The Bank and HM Treasury's priority is to accelerate CBDC development work to be in a position to build a CBDC, in the event that a decision is made to do so.

The functional requirements, technology considerations and illustrative technology model in this paper represent the Bank's emerging thinking on these matters. The technology implications discussed are not exhaustive and will be tested and developed further in the next phase of work.

The Bank's CBDC roadmap

A UK CBDC would be a major project, involving distinct phases of work.

Figure 2: Indicative CBDC roadmap



The digital pound CP and this TWP build on the Bank's previous work on CBDC.

In March 2020, the Bank published **a Discussion Paper on CBDC**. It outlined one possible approach to the design of a CBDC, referred to as the platform model. It also sought feedback from a wide range of stakeholder groups and in June 2021, the Bank published a **summary of the responses**.

In June 2021, the Bank set out possible opportunities and risks in **a Discussion Paper on new forms of digital money**. In March 2022, the Bank published a **summary of the responses**.

The digital pound CP and this TWP represent the conclusion of the 'research and exploration phase' of our work on CBDC. We will now move to the next stage, the 'design phase', to develop, in technology and policy terms, the CBDC model set out in the digital pound CP.

The design phase will equip us to respond to developments in the payments landscape and reduce the lead time, were a decision to be taken to build a CBDC in the future. This will involve investment in the Bank's technology capabilities, an ambitious approach to the technology roadmap and extensive engagement with the private sector.

By the end of the design phase, the Bank intends to have evaluated the technology feasibility of CBDC, determined the optimal design and technology architecture, and supported business model innovation through knowledge sharing and collaboration between the private and public sectors.

Consistent with the Bank and HM Treasury's goal of accelerating the development of a UK CBDC and positioning the authorities to respond to developments in the payments landscape, our aims for the design phase are to:

- cut lead-times on CBDC development and equip ourselves with the knowledge and capabilities to move into a build phase, if required;
- determine the technology feasibility and investment needed to build CBDC;
- articulate, in detail, what the technology and operational architecture for a UK CBDC would look like;
- assess and evaluate the benefits and costs of the CBDC architecture;
- deepen the Bank's knowledge of CBDC technology and support stakeholder understanding of our technology approach;
- support the development of the broader UK digital currency technology industry through collaboration, knowledge-sharing, experimentation and proofs of concept; and
- provide the basis for a future decision on whether to introduce a CBDC and move to a build phase.

Consistent with those aims, the design phase has two focus areas, both aiming to accelerate the development of a UK CBDC.

The first objective of the design phase is to develop a comprehensive, conceptual architecture which can be used as the blueprint for construction of a UK CBDC, should we proceed to a build phase. This will require us to set out in detail the comprehensive and precise requirements for CBDC technology, the architecture and operating model, and high-level rules for participation in a CBDC ecosystem. This will allow stakeholders to understand the Bank's approach to technology, requirements for technology solutions, and the commercial and operational implications of a CBDC.

The second objective is experimentation and proofs of concept, in collaboration with private sector innovators, aims to inform the development of the CBDC architecture and build both the Bank, and the private sector's digital currency technology know-how. The Bank will operate an open and transparent process for participation in proofs of concept and share the lessons learned from those experiments.

The design phase will present opportunities for private sector business model innovation and support technology capability in the UK fintech sector. These are benefits we expect to endure even if we do not proceed to build a CBDC.

The design phase will present benefits for the wider UK fintech community. Technologies for a CBDC are also relevant to privately issued digital money, like stablecoins. By partnering on proofs of concept and experiments, the Bank and HM Treasury seek to catalyse private innovation in digital currency technologies, encourage innovative digital money business models and support knowledge sharing across the UK fintech sector. The design work will also benefit the Bank as supervisor of financial institutions that might seek to use such technologies by helping us to better assess their implications for financial stability and the safety and soundness of PRA regulated firms. Given our expectation that digital currency technologies will be a significant area shaping the future of finance, the benefits of the design phase are expected to endure even if we do not build a CBDC.

After the design phase, there will be a decision on whether to build a CBDC.

On completion of the design phase, following further consultation and in light of the ongoing developments in the payments landscape, the Bank and the Government will decide whether to build a CBDC. Work undertaken during the design phase will help to generate evidence to support a thorough evaluation of benefits and costs.

If we decide to move into a build phase it would involve developing prototype(s) of CBDC technology in a simulated environment, before moving to pilot tests. A CBDC would only be launched if, among other things, it met all our exacting standards for security, resilience, and performance.

A decision on whether to proceed to a build phase could be made around the middle of the decade. The second half of the decade is the earliest a UK CBDC might become operational.

A CBDC would be a major infrastructure project and would require significant investment. Any decision on whether to build one would require extensive evidence gathering, careful evaluation and comprehensive stakeholder engagement. The legal basis for a UK CBDC will be determined alongside consideration of its design.

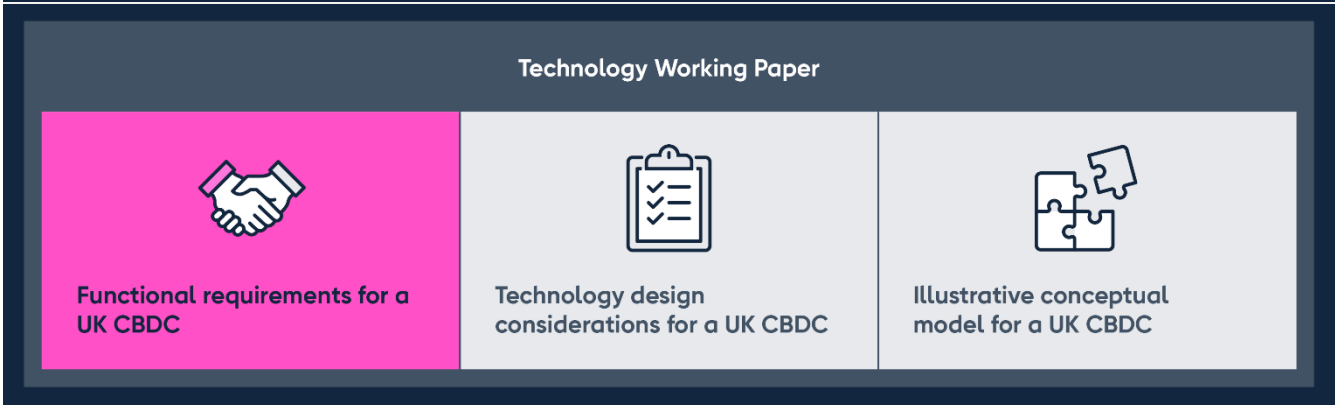
We judge that the second half of the decade is the earliest point at which a CBDC might be launched. It would take time to build infrastructure that is secure, resilient, and high performing. Experience from overseas digital currency projects, and from digital innovation

more generally, indicates that building user familiarity and understanding, and ensuring that innovative and customer friendly applications emerge, will be critical to success.

We will engage stakeholders extensively and be transparent about our work.
Transparency around our work, and engagement with a wide group of stakeholders, will be more important than ever. This will build upon our approach to date, including our **Engagement and Technology Forums**. We will also continue engagement with civil society, academics, technologists, and businesses across the UK.

2: Functional requirements

Figure 3: Overview of the TWP – functional requirements for a UK CBDC



The Bank and HM Treasury's public policy objectives determine CBDC functionality and technology choices.

The design of a UK CBDC must deliver the Government and Bank's policy objectives. The digital pound CP sets out two public policy objectives:[1]

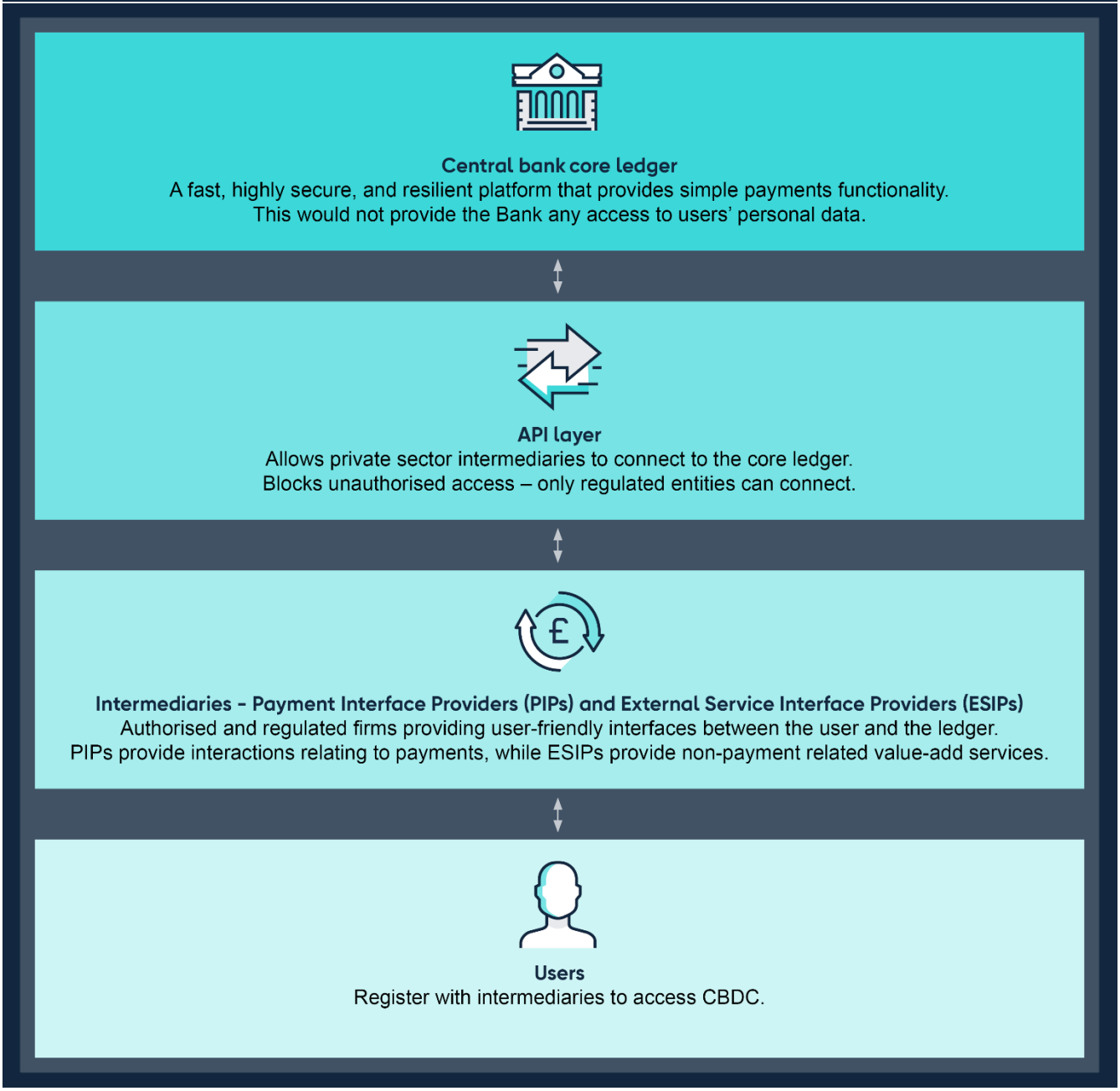
a) To sustain access to UK central bank money – ensuring its role as an anchor for confidence and safety in our monetary system, and to underpin monetary and financial stability and sovereignty; and
b) To promote innovation, choice, and efficiency in domestic payments as our lifestyles and economy become more digital.

The platform model is the proposed model for CBDC.

The digital pound CP proposes that a UK CBDC would be based on the platform model, as originally set out in the Bank's **2020 Discussion Paper**. In the platform model, the Bank would build a fast, secure, and resilient platform – the 'core ledger' – which would provide the minimum necessary functionality for a CBDC. Regulated private firms, Payment Interface Providers (PIPs) and External Service Interface Providers (ESIPs), could then access the core infrastructure via an application programming interface (API) layer.

[1] See Part D of the **digital pound Consultation Paper**.

Figure 4: The platform model



The platform model is based on a public-private partnership.

The platform model specifies the roles and responsibilities of the public and private sector in the provision of a CBDC. The Bank provides the core infrastructure upon which the private sector builds, innovates and delivers value-add services to households and businesses.

PIPs function as gateways to the CBDC ecosystem, offering users digital 'pass-through' wallets[2] to interact with, and manage, their CBDC holdings. ESIPs might provide non-payment, value-add services, such as business analytics, budgeting tools and fraud monitoring.

We expect in-store, online and peer-to-peer (P2P) payments to be the initial focus of a UK CBDC. Over time, a broader range of payments may be enabled.

The digital pound CP proposes that CBDC would be used by households and businesses for their everyday payment needs. As such, upon introduction, the CBDC system would support two essential types of payments, person-to-business (P2B), both in-store and online, and P2P.

Over the longer term, innovation and evolving user needs may mean a broader range of CBDC payment types could be offered. For example, offline and cross-border payments could support public policy objectives, but might take time to deliver given the technological and operational complexities involved. Batch, split, and micropayments are additional payment types that could help to support innovation and meet user needs.

CBDC would be accessed via smart devices and cards.

The digital pound CP outlines how users would interact with their CBDC holdings. Users could access CBDC through wallets on smart devices. This means that they would be able to open a wallet using these devices, which would enable them to manage their balance and make payments. Smart devices might include smartphones, laptops, Internet of Things (IoT) devices and wearables. Not everyone has a smart device or finds it easy to use one, so users could also have physical card options for CBDC payments.

It should be fast and easy to transfer between CBDC and other forms of money, including cash and bank deposits.

Households and businesses currently make payments using a mix of bank deposits and cash. It should be simple, fast and convenient to move between CBDC and other forms of money, particularly cash[3] and bank deposits.

A UK CBDC should implement economic design choices as set out in the digital pound CP.

The digital pound CP sets out economic design choices for a UK CBDC. Two of those choices have particular implications for technology:

---

[2] They are called 'pass-through' wallets as the users' holdings are recorded on the Bank's core ledger, and the wallet simply passes instructions from the user to the core ledger.

[3] The physical nature of cash makes moving between it and other forms of money more challenging than digital money, but it is important that the aim remains to achieve simple, fast and convenient movement. This is likely to require working with existing cash distribution market participants.

First, a UK CBDC would be subject to some limits on individuals' holdings, at least during its introductory period. The technology design should support the implementation of these limits, including, if needed, the ability to change either the design or the level of any limit.

Second, there may also need to be restrictions on corporates' holdings of CBDC. Given that corporates vary significantly in size, transaction volume and the activity they undertake, the design of corporate limits will be subject to further research. Technology solutions, such as balance sweeping, might have applications with respect to limits on corporate holdings by allowing corporates to freely receive CBDC payments, but preventing them from storing value in CBDC in a way which might be detrimental to financial stability by disintermediating critical money markets.

CBDC could offer a broad range of functionalities and features.

Table A below summarises potential functionality and features of a CBDC discussed in the digital pound CP.

Table A: Summary of CBDC functionality and features

Categories	Functionality and features
Payment devices	• Smart devices and physical cards • Existing online and in-store point-of-sale infrastructure • Internet of Things devices • Wearables
Wallet management	• Opening a wallet • Viewing balances
Payments	• Real-time one-off push • Peer-to-peer • Person-to-business (both in-store and online) • Cross-border • Offline • Scheduled • Micropayments • Batch payments, eg wage • Split
Interoperability	• Moving between CBDC and other forms of money, particularly cash and bank deposits

Categories	Functionality and features
Economic design	• Ability to implement limits policy
Identity, data and privacy	• No access to users' personal data by the Bank • PIPs undertake know your customer checks and anti-money laundering (AML) compliance • CBDC would not be anonymous • Potential for users to have privacy controls on wallets • Potential for tiered wallets based on ID information

The payments use cases for CBDC are likely to evolve over time. There will need to be careful consideration of the ability to meet future payment needs which extend beyond those covered in the table.

3: Technology design considerations

Figure 5: Overview of the TWP – Technology design considerations for a UK CBDC

Technology design considerations are a useful way to organise and guide our work. In this section, we explore six technology design considerations which can help organise and guide our technology work. They will likely have significant impact on eventual CBDC design choices. While there are other technology considerations to be taken into account, the Bank considers that these six considerations are priorities and will provide a basis for testing architectures and solutions, and evaluating design trade-offs. These design considerations are:

- Privacy
- Security
- Resilience
- Performance
- Extensibility
- Energy usage

3.1: Privacy

Summary

- Neither the Government nor the Bank would have access to users' personal data.
- Privacy-enhancing technologies might support privacy in the CBDC system while assisting PIPs in complying with legal and regulatory obligations.
- Understanding the application and feasibility of these technologies in supporting our policy objectives requires technology-agnostic evaluation and practical experimentation.

Privacy is fundamental to trust and confidence in the CBDC system.

A UK CBDC would be designed to promote and protect privacy in accordance with users' personal data rights. This is essential for user trust and confidence in the CBDC system. The CBDC system should implement 'data privacy by design' while facilitating compliance with all applicable laws and regulations. The digital pound CP proposes five design objectives related to privacy:[4]

- Neither the Government nor the Bank would have access to users' personal data except for law enforcement agencies under limited circumstances, prescribed in law, and on the same basis as currently with other digital payments.
- CBDC would not be anonymous because the ability to identify and verify users is needed to prevent financial crime and to meet applicable legal and regulatory obligations.
- Users should be able to choose from a range of wallet services. Varying levels of identification would be accepted to ensure that CBDC is available for all.
- Users should be able to vary their privacy preferences to suit their privacy needs within the parameters set by law, the Bank and the Government, as part of system design.
- Enhanced privacy functionality could result in users securing greater benefits from sharing their personal data.

These design objectives inform possible technology requirements for privacy. A provisional set of possible requirements is set out in Table B. These requirements are mapped to principles of the UK General Data Protection Regulation.[5]

[4] See Section D.2 of the **digital pound Consultation Paper**.

[5] **The Data Protection Act 2018**; **The principles.**

Table B: Privacy technology requirements

Privacy technology requirement	Data protection principle
Any information accessed by the Bank would have to be effectively anonymised off-ledger.[6]	Integrity and confidentiality
Personal data collected during user on-boarding and payment transactions should, by default, be limited to that required for those purposes. Users might choose to provide additional data in exchange for advanced services.	Data minimisation Lawfulness, fairness and transparency
Know your customer data collection processes should support integration with user identity services.[7]	Lawfulness, fairness and transparency
PIP and ESIP access to transaction data within the CBDC system should be limited to the legal and regulatory minima, with users controlling their preferences.	Lawfulness, fairness and transparency Integrity and confidentiality Data minimisation
Where PIPs and ESIPs need identity and payments data to be linked, their access to these data must be limited to the legal and regulatory minima.	Integrity and confidentiality Data minimisation Lawfulness, fairness and transparency

Privacy-enhancing technologies

Privacy-enhancing technologies (PETs) show promise in enabling payment and data processing while minimising personal data exposure, and maximising security.

The term PETs covers a broad range of technologies designed to support privacy and data protection. These technologies may be cryptographic, statistical or procedural in nature. Since PETs enable a 'data privacy by design' approach to data processing, they might support the policy objectives related to privacy. Further work is needed before any decision can be made on whether or not to use PETs. In the interim, the Bank has collated a non-exhaustive list of PETs which might have applications in a CBDC system. The merits and case for use of such PETs, along with others not listed here, will be assessed in the next phase of work.

6 **ICO (2021) – How do we ensure anonymisation is effective?**.

7 **HM Government (2016) – 'Know your customer' guidance**; and **HM Government (2021) – UK digital identity and attributes trust framework**.

a) Data minimisation

Data minimisation techniques could give users better control of their data, enabling them to choose which data they share with PIPs and ESIPs. Some techniques include:

- Pseudonymisation, which is a procedure that removes information that identifies an individual and replaces it with pseudonyms. Proposed amendments to current data protection legislation require that the pseudonymised data be kept separately from identifying data. Pseudonymisation might be used by PIPs and, in some cases, ESIPs, to protect user personal data in storage and transit.

- Private information retrieval (PIR), which allows a party to search for and retrieve data records from a database, without revealing details about the query or the result to the data controller. PIR might allow users to search for and retrieve their account information without revealing the search parameters and results to their PIPs.

- Attribute-based encryption (ABE), where the ability to read encrypted data is determined by attributes, such as the account ID or email address. The ciphertext and decryption key in ABE are labelled with user attributes, such that decryption is dependent on a match between the attributes of the ciphertext and the decryption key. ABE might be used to secure the transfer of transaction data between users, PIPs, and the Bank, with the ability to decrypt data determined by user attributes of the transaction recipient.

b) Aggregate data analysis

Aggregate data analysis supports the processing of such data, while minimising or avoiding the exposure of personal data. Some techniques include:

- Differential privacy, which introduces statistical noise or randomness to data sets. The calculated injection of noise hides personal data and might enable analysis of group patterns in a data set.

c) Distributed data analysis

Distributed data analysis refers to the processing of distributed data sets by multiple parties in a privacy-preserving manner. Some techniques include:

- Secure multi-party computation (SMPC), which enables multiple entities to jointly process or perform calculations on distributed datasets without sharing data with each other. This technique could minimise sensitive data sharing in the ecosystem and

ensure that no single entity can see the entire dataset. SMPC might enable PIPs to monitor transactions for money laundering with minimal sharing of data.

- Federated learning, which is a machine learning (ML) technique used across distributed datasets that are held locally by multiple entities. Federated learning might allow PIPs to locally monitor transactions for money laundering, with suspicious events flagged and pushed out to the relevant PIPs. This technique eliminates the need for data sharing in the ML model training process and could be used in combination with other PETs to protect user privacy.

d) Encrypted data processing

Encrypted data processing allows one party to process data held in encrypted form by another party. Some techniques include:

- Homomorphic encryption, which allows parties to process encrypted data without first having to decrypt it. The data remain encrypted at all times, reducing the likelihood of sensitive data disclosure or information compromise in the ecosystem. This technique might help PIPs share and process sensitive data in a privacy-preserving manner, for example for anti-money laundering (AML) compliance.

e) Blind proofs

Blind proofs can be used to verify claims about data without having visibility of the data. Some techniques include:

- Zero knowledge proofs (ZKP), where one party can prove to another party that a given statement is true without revealing any additional data apart from the fact that the statement is indeed true. Where a user holds multiple wallets across PIPs, ZKPs might be used by PIPs to verify that a user's CBDC holdings are within set holding limits, without requiring visibility of funds held by the user across wallets. ZKPs might also be used by a PIP to attest to completion of know your customer (KYC) checks without exposing personal data to the Bank and other ecosystem participants.

- Zero knowledge range proofs (ZKRP), which are used to verify that a secret value is within a certain range. ZKRPs might be used to verify whether CBDC funds are within a set holding limit for the user, without exposing the user's balance.

Where the application of PETs to support a data privacy by design approach is deemed necessary or useful, further work will be required to determine the circumstances in which the Bank, PIPs or ESIPs might apply them. The Bank will assess the suitability and feasibility of PETs in supporting the Bank and HM Treasury's policy objectives related to privacy. This assessment will be agnostic with regards to other technology and architectural choices for

CBDC, and will include exploring the scalability and performance potential of PETs in a range of architectures.

PETs may introduce varying degrees of system complexity.

Greater levels of transaction privacy require increased protection of personal data. Data protection might be achieved using traditional access management mechanisms or novel cryptographic privacy technologies, including PETs.

PETs are likely to introduce system complexity to varying degrees. This could create a tension with security, performance, resilience, interoperability and extensibility requirements, as well as with system build and operation costs. The Bank does not intend to receive or use personal data. This might minimise these trade-offs at the level of the core ledger, but as a consequence data anonymisation must take place off-ledger. Further work is needed to assess the technology implications of such an arrangement.

The complexity and efficiency of potential PETs in the CBDC ecosystem depends, to an extent, on existing trust relationships between ecosystem participants. Future assessment of the expected trust relationships between the Bank, PIPs, ESIPs and users, might guide the assessment of where in the ecosystem these technologies might be applied.

Adoption of new or advanced cryptographic technologies could also introduce software or protocol-level security risks. Where bespoke system components and technologies might be used in the CBDC system, these must be designed and built in accordance with stringent standards and assurance principles.

Next steps

The Bank plans to examine, during the design phase, the suitability and possible application of PETs for enabling privacy in transactions and data processing activities. That will include conducting tests and evaluating the legal, technical and operational standards needed to deliver privacy and ensure that the Bank does not have access to personal data.

Further technology work will aim to identify the design implications and challenges with various privacy technologies, as well as the use of multiple technologies in combination.

3.2: Security

Summary

- A CBDC system that is secure by design ensures confidence in money and promotes user trust and adoption.
- Security risks for a CBDC system are largely the same as for other retail payment infrastructure, but additional functionality, such as offline payments and programmability, could introduce new and additional security risk.
- As national infrastructure, it is crucial that security risks are evaluated early in the design phase, and security controls are designed and built into the CBDC ecosystem, alongside stringent and comprehensive risk assurance and management.
- A resilient, layered security design that assumes breach could occur will help minimise the likelihood of a threat actor advancing within the CBDC system.
- The Bank is working with partners to understand different approaches to threat modelling and system-driven security risk management.

The security of the CBDC system is fundamental to the trust and confidence placed in it.

As national infrastructure, the CBDC system would be a potential target for cyber threats. Threat actors, with developed cyber capabilities and an intent to compromise, present a threat to the security and continuity of CBDC system operations. Those targeting CBDC could include criminals and nation state actors, activists and terrorists, with the insider threat sitting across all of these categories. Each of these threat actors have different motivations and cyber capabilities. Access to an insider would immediately increase the capability of any other category of threat actor.

Nation states represent the greatest threat to security as they have the motivation and capability to compromise a variety of technology infrastructures. Nation states are also more likely to invest time and resources in attempting to exploit potential vulnerabilities, either directly or through the system's supply chain. While the nation state threat is limited to a few adversarial states, their motivations could range from disrupting the operations of the CBDC system, to gathering intelligence to further their own research and development capabilities.

Criminals are more likely to target the CBDC ecosystem through fraud and ransomware. A CBDC could also attract more sophisticated organised crime syndicates with illicit finance interests, such as theft and money laundering. The Bank acknowledges this threat, and were

a CBDC to be launched, would work with private sector partners, including PIPs and ESIPs, to manage this risk while protecting user privacy.

A successful attempt to breach a CBDC system might impact users' holdings and their ability to make payments. This might, in turn, affect confidence in money and trust in, and adoption of, a CBDC. Attacks might also target end-users, which is seen as payment fraud in current retail payment services. This is commonly independent of the security of the system. The public's security awareness is therefore a very important factor.

The Bank acknowledges that defending a retail CBDC system would be more complex than securing wholesale systems, such as the Real-Time Gross Settlement (RTGS) service. This is due to the number of intermediaries and end-users in a high-volume retail system, which increases the attack surface. Therefore, were a CBDC to be launched, the Bank would work closely with partners to ensure that security risks are identified and managed across the CBDC system.

Security threats would largely be the same as for other retail payment infrastructure, but innovative functionality may present new and additional risks.

Like any other retail digital payment service, a CBDC system could be subject to payment fraud, cyber risk, operational risk, and supply-chain security and concentration risks.[8] If not effectively managed, these risks could impact the confidentiality, integrity, availability and authenticity of the system. Crystallisation of these risks might have financial and operational impacts for users, affecting their confidence and trust in money, and could cause reputational damage to the Bank. These impacts might include data compromise, system outage or tampering with funds. Failure or compromise of a CBDC system could also impact connected payment services. Macro-level weaknesses, such as single point of failures in infrastructure and critical service providers, system integrations and data dependencies, might transmit and amplify incident impact downstream.

The digital nature of CBDC means that funds could be spent more than once. This is also known as the double spend risk. The risk of double spend is more acute for offline payments, which take place disconnected from the core ledger, making it more challenging to verify that funds have not already been spent (Section 4.8).

CBDC should support innovations, such as programmability (Section 4.7), but these could increase security risks and be susceptible to potential software vulnerabilities in code. Therefore, it is important that security is designed into the CBDC system to account for and minimise the likelihood and impact of these risks, while balancing system usability.

[8] **Evans (2022) – How FSI organisations should balance supply chain and concentration risk**.

Threats may evolve during the potential design, build and operational lifetime of the CBDC system. New threats aimed specifically at CBDC might also emerge.

Threats generally evolve and adapt to technology innovation, and to changes in user preferences and behaviour. Quantum computing is one such threat. Quantum computers could provide speed, efficiency, and significantly more processing power than conventional computers. These advances could pose risks to conventional cryptography widely used to secure data and systems today. Table C outlines some of the possible risks that might be posed by a viable quantum computer.[9]

Table C: Possible quantum computing risks and mitigations

Quantum risk description	Possible risk mitigations
Identity compromise; data tampering; and payment fraud Threat actors with access to a public key and a viable quantum computer might derive the corresponding private key and:[10] a) impersonate the key owner, forging their digital signature and authorising spending of funds; and/or b) tamper with information whose authenticity is protected by a digital signature, compromising the integrity and authenticity of payment data.	**Minimise public key exposure** A design that uses a one-way hash of the user's public key reduces the likelihood of signature forgery: a) Key pairs could also be cycled as a way to limit public key exposure. **Key inventory and monitoring of key lifetime** High-value, root-level public keys could be deployed with careful consideration of the key lifetime: a) Keys in use could be inventoried, allowing for a quick migration to a quantum-safe state.
Disclosure (decryption) of volume payment data Threat actors might collect volume-encrypted data anticipating decryption in the near future. As such, a viable quantum computer could present a threat to the security of payment and personal data stored at scale.	**Increase key size** Where encryption methods for symmetric encryption algorithms remain viable, key sizes for long-dated certificates could be increased.

[9] Current quantum computers are highly sensitive to electrical interference and suffer from relatively high computing error rates. Quantum computing is reported to require further development to be productionised, and a viable quantum computer is expected by 2030. **McKinsey (2021) – Quantum computing use cases are getting real–what you need to know**.

[10] Threat actors with access to future viable quantum computers are likely to be nation states. Their prime target would likely be systemic disruption, rather than financial crime and fraud. Nevertheless, these risks have been tabulated as the future state and availability of quantum computers is an unknown today.

In recognising these future risks, the Bank also acknowledges that cryptography primitives break or become obsolete over time. Therefore, the quantum computing threat is an additional layer of risk that the Bank must factor into its CBDC design thinking. The Bank will work with partners to better understand the future risks posed to CBDC by quantum computing.

As CBDC infrastructure would be long-lived, crypto-agility would be a design goal for a CBDC ecosystem. A crypto-agile system supports the rapid adoption of new cryptographic primitives with minimal impact to system infrastructure. For example, crypto-agile public key certificates might simultaneously contain two sets of public-keys: traditional and quantum-safe. These enhanced certificates might allow CBDC ecosystem participants to gradually transition their infrastructures and systems to a quantum-safe state, while maintaining backward compatibility with legacy systems.

The security of the CBDC ecosystem is grounded in protecting the confidentiality, integrity and authenticity of user and payment data, and the availability and secure access management of the systems on which that data resides.

Cyber-attacks launched by advanced persistent threats typically involve the establishment of a persistent foothold on internet-connected systems, lateral movement across the ecosystem, and finally escalation of access privileges.[11] In a CBDC ecosystem, the initial point of compromise might be PIP and ESIP infrastructure with internet connectivity. This would likely be followed by attempts to maintain and widen system access via lateral movement techniques.[12] Once privileged access to a target system hosting sensitive data is achieved, the system might be scanned for vulnerabilities that can be exploited in a range of attacks impacting confidentiality, integrity, availability and authenticity. These four foundational attributes of data and system security are defined below in Table D.

[11] **Advanced Persistent Threat**; **Principles of Defence and Offense.**

[12] **NCSC (2018) – Preventing Lateral Movement**.

Table D: Security attributes

Security attribute	Description
Confidentiality	Confidentiality is about ensuring that sensitive personal[13] and non-personal data is only made available to ecosystem participants on a need-to-know basis. Confidentiality of data helps to protect against the following: • Loss of data from the CBDC system • Loss of user confidence in the CBDC system
Integrity	Integrity refers to protecting against unauthorised modification, appropriation or destruction of user funds and sensitive data, and that of the systems on which they rely. Integrity of data and systems helps to protect against the following: • Manipulation of data in the CBDC system • Loss of funds • Loss of user confidence in the CBDC system
Availability	The continued availability of the CBDC core ledger and wider ecosystem is integral to system resilience. Availability of data and systems helps to protect against the following: • User inability to access funds and data • Loss of user confidence in the CBDC system
Authenticity	Authenticity of the CBDC ecosystem relates to its protection from spoofing[14] and repudiation attacks.[15] Authenticity of data and systems helps to protect against the following: • Repudiation of user activity • Unauthorised access to data in the CBDC system • Double spend of CBDC • Loss of user confidence in the CBDC system

[13] Sensitive CBDC data includes user identity data captured for KYC purposes, and CBDC holdings and transaction payment data in the CBDC ecosystem. The core ledger would not hold or access personal data.
[14] Spoofing is the act of disguising a communication or identity so that it appears to be associated with a trusted, authorised source.
[15] A repudiation attack involves the malicious manipulation or forgery of user activity. The issue of repudiation is concerned with a user denying that they performed an action.

Secure access management, including user and system authentication and authorisation, is therefore central to upholding a minimum baseline of security.

The provision of user services by PIPs and ESIPs promotes a competitive ecosystem for CBDC, but extends the potential attack surface to these intermediaries.

The retail focus of CBDC, and the internet-facing nature of the wider ecosystem, increases its attack surface. A compromise in the security of a PIP or an ESIP might enable an attacker to extend access to connected core ledger infrastructure, and access or tamper with data or disrupt system operations. This could potentially lead to a loss of system integrity, a confidentiality breach or data breach, or the unavailability of the CBDC system and user funds.

The security and resilience capabilities and controls of PIPs and ESIPs should be assessed and suitably risk managed via a security assurance programme. This should occur at the point of onboarding each intermediary, and throughout its lifecycle. The Bank anticipates that such a programme would align with any applicable regulation, and security assurance and operating standards, which might in turn determine security expectations for PIPs and ESIPs. The security and resilience aspects of the CBDC system will be considered simultaneously in the design phase.

Providers of networking, messaging, hardware, and software services to CBDC ecosystem participants are important to the security of the CBDC system.

The CBDC ecosystem would be composed of a network of service providers and consumers. Supply chain attacks typically target a trusted third-party service provider, vital to ecosystem operations, as recently seen in the Log4J vulnerability.[16] Service providers in the ecosystem might be the victim of a supply chain attack, and the compromise of a critical service provider might even result in a systemic incident. A systemic incident occurs at the point at which the financial system is unable to absorb the impact of disruption. A cyber incident may become a systemic incident if it moves from presenting an operational risk to eroding trust and confidence in the financial system.

There are a number of measures to manage supply chain risks. These include secure design approaches with consideration for third-party providers that might present a single point of failure, governed frameworks enforcing adequate management of supply chain risks, and consideration of scenario-based cyber stress testing involving CBDC intermediaries.

A decision to build a CBDC would require a detailed analysis of current and future threats in order to manage ecosystem risks.

While the Bank would be responsible for managing the security of the core ledger and API layer, other ecosystem components would be owned and operated by PIPs and ESIPs. PIPs and ESIPs would be responsible for managing the security of their own components.

---

[16] **Supply chain attack examples**; **Log4j vulnerability – what everyone needs to know**.

Regardless of system ownership, the Bank would be exposed to reputational damage arising from an attack or system failure impacting the confidentiality, integrity, availability, and/or authenticity of CBDC infrastructure, data and funds. The Bank would therefore take a close interest in, and set expectations for, security standards for the wider CBDC ecosystem.

Layered security is one approach to managing threats to the CBDC ecosystem. This approach assumes the existence of threat actors in the ecosystem and uses multiple layers of security controls aimed at detecting and preventing lateral movement by threat actors. Iterative system-driven risk management can also be important in identifying, evaluating and assessing risks to the end-to-end CBDC system, and managing these against a defined risk appetite.[17]

The security of the CBDC system would need to be assured, from design and development to through-life assurance, once launched. Through-life assurance could include vulnerability management, security testing and exercising with PIPs and ESIPs, security audits and other supplier assurance considerations.

Regulation helps to manage ecosystem technology risks in existing payment infrastructure today.[18] Further work is required to understand the regulatory model relevant to the potential development of the CBDC ecosystem, and how this can support end-to-end security in a CBDC system.

A balance between security and other system requirements is essential in designing and building a CBDC system that is trusted, high-performing and easy to use.

Controls that secure access to data, such as data encryption and user authentication, typically have a negative impact on transaction processing time. Additionally, while the layering of security controls is good practice and highly recommended, controls providing defence in depth must be assessed for their impact on system performance, usability and cost. Consequently, security controls must be carefully selected in a manner that meets security requirements without negatively impacting core system functionality and other desired system characteristics.

[17] **NCSC (2017) – Risk management guidance**.

[18] For example, the Strong Customer Authentication (SCA) requirement under the Payment Service Directive (PSD2) reduces the risk of fraud. **Using GOV.PAY**; **Payment Services Regulations 2017**; **EBA (2019) – EBA Guidelines on ICT and security risk management**.

Next steps

The Bank will continue to work with partners to understand potential approaches to threat modelling and system-driven security risk management for use in identifying and managing CBDC security risks.

When evaluating possible CBDC designs, the Bank will conduct a prospective system-driven security assessment of any possible CBDC system to produce a comprehensive set of security requirements.

The Bank also plans to work with partners to undertake research into future threats, such as quantum computing, and evaluate options for a quantum-safe CBDC ecosystem. That work will include producing a framework for evaluating and managing new and emerging risks.

Further work is also required to assess how security assurance and regulatory oversight might be achieved without impacting participation and diversity of PIPs and ESIPs in the CBDC ecosystem.

3.3: Resilience

Summary

- A CBDC system that is resilient to disruption ensures the availability and integrity of data and supporting systems.
- The balance between CBDC system integrity and availability is a key consideration, and needs further research and analysis.
- Current RTGS and CHAPS services have a target uptime of at least 99.95%, and that would constitute a minimum expectation for Bank-managed CBDC infrastructure. However, we will explore whether an uptime target of closer to 100% would be appropriate and deliverable (in particular 99.999%).
- Uptime targets are only one element of payment system resilience and this target would be complemented by best practice risk management processes and controls.

A resilient CBDC system supports the Bank's financial stability objective.

As retail payment infrastructure, the availability of the CBDC system for payments processing is critical, as is the integrity of its data. Disruption to payment processing or a loss of data integrity could lead to financial loss, and threaten user confidence. Sustained downtime or a breach of CBDC system integrity could also affect connected payment services. This could be detrimental for financial stability. Therefore, it is essential that security and resilience principles are designed into the fabric of the CBDC ecosystem.

The risk of disruption must be suitably managed to minimise the likelihood of occurrence, as well as to mitigate and recover from any disruption that might occur. A resilient system promptly detects, responds to and recovers from disruption, and effectively protects its critical services. Resilience against operational risks would help to ensure that any incidence of disruption to the CBDC system does not affect financial stability.

A resilient service, enabled via containment and redundancy mechanisms, ensures that any disruption is minimal and short-lived.

Containment mechanisms aim to reduce the scope and impact of system disruption. Identifying and minimising strong dependencies between system components that could allow errors to propagate around the system is key to containing the impact of a disruptive event. Where dependencies between CBDC system components are essential for system operations, orderly shutdown mechanisms should be employed.

Redundancy mechanisms, such as orderly shutdown, switch from normal service mode to a well-defined contingency mode to reduce the risk of contagion to data or system integrity. It also enables service recovery in a controlled manner once the fault is contained. An alternative strategy might be orderly degradation of system performance, where core

services continue to operate but at reduced capacity. These redundancy mechanisms ensure that the system as a whole can continue to operate business-critical services in contingency mode until full system recovery.

Resilience is grounded in the system's ability to anticipate, detect, withstand, respond to, recover from, and adapt to, disruption.

Standards might be established to ensure that the CBDC system can efficiently anticipate, detect, withstand, respond to, recover from, and adapt to disruption. The CBDC ecosystem design should account for these five phases of the system resilience lifecycle (Figure 6).

The Bank, as well as PIPs, ESIPs and critical service providers[19] in the CBDC ecosystem, would need to identify the important business services for their operations,[20] the dependencies between these services, and set impact tolerances for each.[21] The identification of important business services and the dependencies between them is essential for understanding and evaluating risk concentration, and minimising risk in design. The Bank and other CBDC ecosystem entities would also need to identify and address risks to their ability to remain within set impact tolerances.

[19] Financial services firms and financial market infrastructure firms are increasingly relying on third parties outside the finance sector for key functions or services (eg cloud-based computing services) through outsourcing and other arrangements. Where many firms rely on the same third party, the failure or disruption of this 'critical' third party could threaten the stability of, or confidence in, the UK financial system. **HM Treasury (2022) – Critical third parties to the finance sector: policy statement**.

[20] An important business service is defined as one where a prolonged disruption of the business service could significantly threaten the transfer of payments or the safety and efficiency of the payment system. **Bank of England (2021) – Operational Resilience: Recognised Payment System Operators and Specified Service Providers**.

[21] Impact tolerance is the maximum tolerable level of disruption for an important business service, whereby further disruption could significantly threaten the transfer of payments or the safety and efficiency of the payment system. **Bank of England (2021) – Operational Resilience: Recognised Payment System Operators and Specified Service Providers**.

Figure 6: System resilience lifecycle

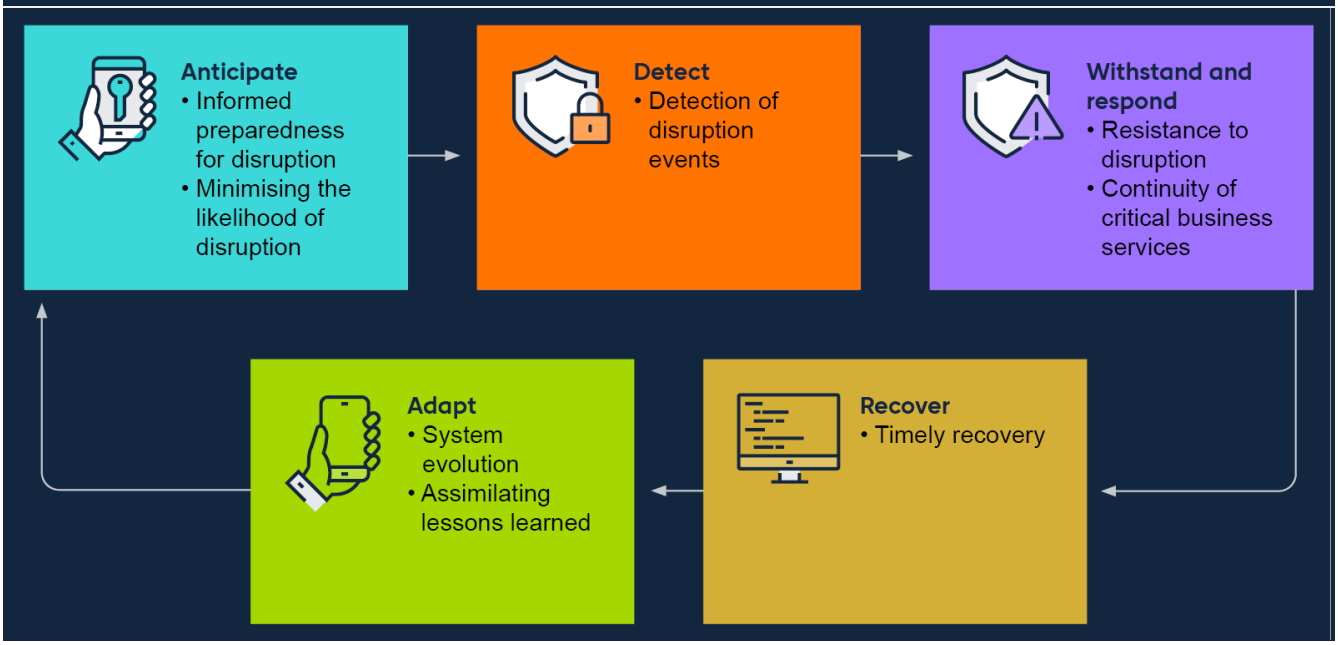


Table E below sets out the potential requirements for resilience and maps these requirements to each of these five phases.

Table E: Resilience requirements for a UK CBDC

Resilience requirement	Resilience lifecycle phase
The CBDC system must be operational 24/7/365. As a retail payment infrastructure, the CBDC service would be available to end users 24 hours a day, every day of the year. Planned upgrades and maintenance should not affect service availability.	Anticipate Withstand and respond
The CBDC system must have a very high degree of availability. Although capable of operating 24/7/365, CBDC might, in very rare circumstances, be subject to outages or disruption, much like existing retail payment services. CBDC must be designed to minimise or avoid service interruption. Uptime is the time that a system is available and operational. Current RTGS and CHAPS services have a target uptime of at least 99.95%,[22] and that would constitute a minimum expectation for Bank-managed CBDC infrastructure. However, we will explore whether a standard tailored to retail payments, where uptime targets are typically closer to 100%, would be appropriate and deliverable (in particular 99.999%). Uptime targets are only one element of payment system resilience, and	Anticipate Withstand and respond

[22] Bank of England (2022) – Real-Time Gross Settlement (RTGS) system and CHAPS Annual Report 2021/22

Resilience requirement	Resilience lifecycle phase
this target would be complemented by best practice risk management processes and controls. There could also be minimum uptime requirements that PIPs and other service providers might need to meet.	
End-users might be able to process some payments in the event of unavailability of the core ledger. A CBDC with offline payment functionality could provide additional system resilience in a very rare circumstance where the core ledger is unavailable. But this would pose a range of technological, operational, policy and legal challenges, including liability for any failed or fraudulent transactions while offline.	Anticipate Withstand and respond
The CBDC system must be able to detect disruptive events. A resilient CBDC must be able to detect disruptive events which could impact the delivery of critical operations, in order to support subsequent response and recovery. Key performance indicators, such as ‘mean time to detect’, are an important design consideration for detection mechanisms that contribute towards ensuring a timely service recovery.	Detect
The CBDC system must be fault-tolerant. Fault tolerance is the degree to which a system operates as intended, by minimising the impact of disruption during the failure event. Fault tolerance is achieved using containment and redundancy controls. A fault-tolerant CBDC is able to detect, respond to, and recover from, faults.	Detect Withstand and respond Recover
The CBDC system must be able to continue safely with critical operations in the event of disruption. The CBDC system must be resistant to disruptive events, and be able to continue critical service operation until full system recovery. Critical services in the CBDC system must be defined, and continuity plans established and maintained, to ensure safe continued operation in the event of disruption.	Withstand and respond Recover
The CBDC system must be able to respond to disruptive events. On containment of a detected event disrupting CBDC system operations, the Bank must be able to communicate with impacted ecosystem participants to co-ordinate incident management.	Recover

Resilience requirement	Resilience lifecycle phase
The CBDC system must be able to recover from disruptive events. Service recovery is typically associated with a fallback to the primary site of operation. The definition of recovery metrics, such as Recovery Time Objective[23] and Recovery Point Objective,[24] would play an important role in the design of a resilient CBDC system.	Recover
The CBDC system should have trusted data backups to aid in recovery. A core ledger backup might be used for data reconciliation in the event of disruption at one or more entities in the ecosystem.	Recover
The CBDC system must be extensible to enable fault fixing and system updates. A modular architecture supports the application of timely updates to incorporate lessons learned, without impacting normal service operation.	Adapt

A resilient system that incorporates redundancy by design supports high availability requirements, but comes with a cost trade-off. System resilience design choices might also impact the security of the CBDC ecosystem.

A redundant design involves the use of additional infrastructure to act as a backstop in the event of failure or an attack. This redundancy supports the continuity of critical services but has a design trade-off in operating costs.

Decentralised designs based on distributed ledger technology (DLT) might offer resilience and availability benefits, but the increased number of ecosystem entities participating in system governance could increase the system attack surface. The implementation of security controls to minimise these access control risks might impact system performance, and its usability and adoption. Aspects of DLT might be useful in delivering resilience in the CBDC system, although further analysis is required.

Additionally, functionality that provides payment resilience benefits could in turn introduce security risks. The introduction of offline payments for payment resilience in the event of network disruption introduces the double spend risk (Section 4.8).

[23] **Recovery Time Objective**.
[24] **Recovery Point Objective**.

Next steps

During the design phase, the Bank will assess and then seek feedback on comprehensive resilience requirements for Bank-managed infrastructure. That will include analysis of the design prioritisation between system integrity and availability.

The Bank plans to analyse the feasibility of, and the potential challenges in, attaining the potential resilience metrics for Bank-managed infrastructure. That will involve examination of ledger designs that support these resilience outcomes, as well as the optimisation of system availability in response to future user needs.

Definition of resilience requirements for PIPs and ESIPs, and an evaluation of the associated impact on ecosystem business models is also likely to be required as part of the evaluations undertaken during the design phase.

Considerations for how the Bank, PIPs, ESIPs and critical third parties in the CBDC ecosystem could minimise the likelihood of disruption, mitigate its impact and recover from a disruptive event will also be evaluated. This might include using a risk assessment framework to identify operational risks and disruption impacts, and the mitigants to protect against these.

3.4: Performance

Summary

- The Bank estimates that approximately 30,000 transactions per second may be the necessary level of performance needed for a UK CBDC.
- However, as innovation occurs and potential CBDC use cases develop, demands on CBDC throughput may increase. Therefore, the Bank will also explore more ambitious capabilities of up to approximately 100,000 transactions per second.
- In addition to transaction capacity, performance also needs to take account of transaction speed. The ability to process and settle transactions in in under one second appears necessary.

As retail payment infrastructure, CBDC will need to meet exacting performance requirements in terms of speed, capacity and certainty.

A CBDC system would need to handle a high number of transactions to accommodate peak demand, alongside confirming and settling transactions as quickly as possible.

While requirements for throughput and speed will differ depending on the specific CBDC use case and payment type, the Bank will examine solutions for enabling a high-performance CBDC system. An example of how requirements differ by use cases is set out below:[25]

Example use cases

- If using CBDC to pay in-store, fast authentication and transaction time is important. Transactions that confirm within a couple of seconds would suffice for this purpose.
- If using public transport, speed becomes even more important. For example, when paying at a ticket barrier, confirmation speed may need to be under a second to prevent queues and congestion.

[25] Current card payments for some public transport scenarios do not involve transactions being authorised in real-time. In these scenarios, the transit operator and card issuer may share the liability for any unauthorised transactions. CBDC payments might be different, in that all payments would need to be authorised in real-time, thereby making transaction speed an important consideration. There may also be other complicating factors with public transport, for example the journey cost being unknown at the outset, and the application of daily price. **UK Finance (2017) – Contactless Transit EMV Framework**.

Transaction speed of under one second for a standard single destination payment appears necessary.

Some categories of payments would require a faster transaction speed than others. CBDC payments may need to confirm in under one second in order to accommodate all of these categories. Confirmation and settlement of transactions in under one second is possible, but when combined with a high volume of transactions in a production environment, it might present challenges for the performance and capabilities of the core ledger. The Bank plans to examine different technology choices, including those relating to ledger technology, to understand the extent to which they can deliver on our likely requirements for transaction speed.

Throughput of approximately 30,000 transactions per second may be necessary. The Bank will also explore a more ambitious capacity of approximately 100,000 transactions per second, in order to accommodate future payment needs.

The Bank estimates that throughput of approximately 30,000 transactions per second might be needed for a viable CBDC system. This capacity would allow for enough capability to support all retail transactions in the UK on any given day. It would also provide flexibility to cater for an increase in transaction volume over time, alongside supporting the addition of further payment types, such as wage payments and foreign exchange.

However, as potential CBDC use cases develop, CBDC throughput demands may increase. The Bank will assess ledger designs that accommodate much higher capacity, including exploring whether it is feasible for a production system to reach up to approximately 100,000 transactions per second.

A CBDC system should be capable of scaling to accommodate increases in payment volume without negatively impacting overall performance.

Scalability is an important aspect of performance. The use cases for CBDC may evolve over time. For example, functionality, such as micropayments, might increase throughput demands. Therefore, it is important that any CBDC system is built in a way that caters for such increases in demand.

Vertical or horizontal scaling should be considered to ensure that the core ledger is able to accommodate future demands and use cases.

Vertical scaling, whereby computational power of the existing infrastructure is upgraded, is one method to cater for increased payment volume. Horizontal scaling is an alternative, where more machines are added to the resources responsible for payment processing. Generally seen as more desirable, horizontal scaling should be considered in the system design to ensure that the core ledger is capable of accommodating the addition of new computational resources.

Multi-destination and offline payments may be other techniques used to accommodate higher payment volumes in the CBDC ecosystem.

Enabling multi-destination payments would also support future payments use cases. This might include allowing one payment initiation to be split across multiple recipients. Where one API call instructs multiple payments, it could help to ease the performance burden of high payment volumes.

Offline payments might also help to scale transaction capacity. An offline payment would not involve immediate interaction with the core ledger, theoretically allowing higher payment volumes to occur locally without any computational resource. However, enabling offline payments also poses significant challenges (Section 4.8).

Next steps

The Bank will continue to evaluate the performance requirements of a CBDC system, and the technology solutions that might deliver those aims. This will include experimentation of architectures that might meet these performance targets.

3.5: Extensibility

Summary

- CBDC must be extensible to support innovation and future payments needs.
- Extensibility would allow CBDC to expand and enhance its functionality without impacting existing services.
- There are a number of factors that determine extensibility, and the Bank will continue to research how it can be maximised.

The CBDC system will need to support future payment needs and evolving use cases.

The CBDC system must be capable of meeting the needs of a rapidly changing payments landscape, and be able to adapt to innovation and new use cases. In addition, the design of a CBDC should support the services that PIPs and ESIPs develop as their business models evolve.

Extensibility refers to the extent to which a system allows for the addition of new functionality, or the modification of existing functionality, without impairing existing system functions. An extensible CBDC system would be able to expand or enhance its functionality without impacting the existing components.

The following factors might be taken into account in the design of a CBDC system in order to maximise extensibility:

a) Open architecture

The CBDC architecture should be able to add, upgrade or replace components in a smooth manner. This might be aided by:

- using commonly accepted standards, including, where appropriate, open technology standards;
- making use of scalable and upgradable components;
- prioritising portable components;
- clearly defining platform boundaries, like APIs, that serve as an interface between the CBDC system and consumers of CBDC services; and
- establishing robust API governance and version management that supports API changes over time.

b) Composability

A greater degree of extensibility in the CBDC system might be achieved by designing a composable architecture. A composable architecture focuses on defining building blocks that

can be combined to achieve the required functionality of the CBDC system. This represents a move away from inflexible monolithic architectures.

The building blocks of a composable architecture should be designed in a way that ensures they can also be reused for other purposes, extending the functionality of the CBDC system and supporting innovation. When designing the CBDC system's architectural components, the reusability of each module must be taken into account; avoiding highly customised individual components, and instead optimising for flexibility, where possible.

c) Open source

The number of open-source technology initiatives continues to increase. In principle, most open-source products have considered from the outset the modifiability and extensibility of their architectures and components. But in determining whether open-source components are suitable for CBDC, the Bank would also need to consider other factors, such as implications for security and system resilience.

d) Third-party dependencies

Third-party dependencies could impact the extensibility of the CBDC system. This could take the form of limitations brought about by reliance on third-party products, including during routine maintenance and service upgrades. Therefore, implications for extensibility must be taken into account when considering the use of any third-party products to build or operate a CBDC system.

Next steps

During the design phase, the Bank will examine how extensibility might be achieved in the CBDC system. That will include assessment of the appropriateness of using open-source components and approaches.

3.6: Energy usage

Summary

- CBDC infrastructure should be energy efficient and designed in a way which minimises any impact on the environment.
- A UK CBDC would not use the energy-intensive technologies used by some crypto assets.

CBDC should be designed to be energy efficient and to minimise any impact on the environment.

The Bank would design CBDC to deliver the Bank and HM Treasury's policy objectives while seeking to minimise its impact on the environment. The physical effects of climate change and the transition to a net-zero economy can create financial risks and economic consequences. These risks and consequences can affect the safety and soundness of firms, the stability of the financial system and economic outlook.

As new payment infrastructure, the CBDC design could potentially have an impact on long-term goals to reduce demand for energy. Therefore, any Bank-managed infrastructure would need to take an energy efficient approach and make use of renewable energy. At the very least, CBDC would be designed to meet the energy efficiency targets for existing payment infrastructure. In the design phase, the Bank will evaluate the CBDC architecture and components and their energy efficiency holistically.

A UK CBDC would not use the energy-intensive technologies used by some crypto assets.

A UK CBDC would be fundamentally different to a crypto asset. It would not use the energy-intensive technologies, such as proof of work,[26] that underpin some crypto assets.

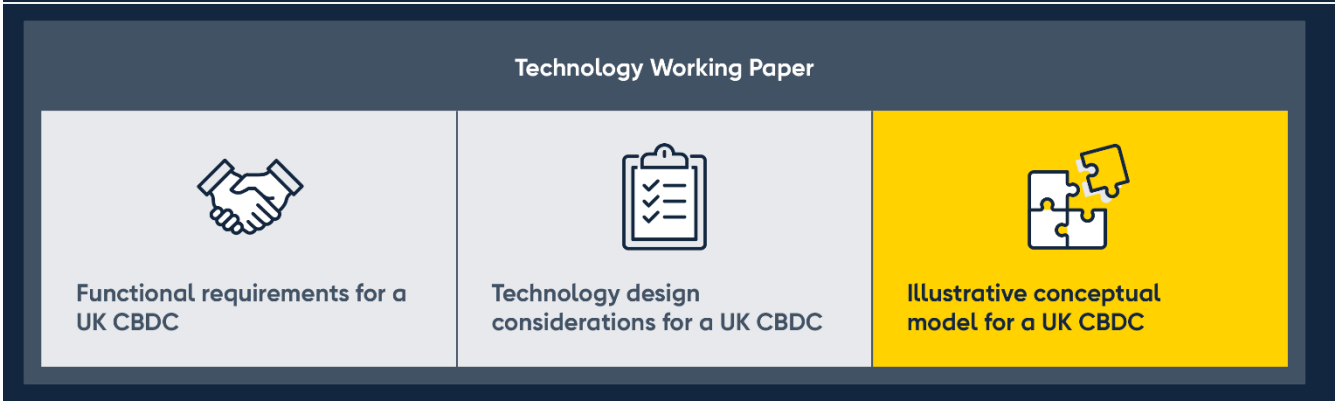
Next steps

During the design phase, the Bank will evaluate the environmental impacts of architectures and components considered for any CBDC system. That will include engaging with stakeholders and experts to establish comprehensive non-functional requirements related to environmental impact and energy efficiency.

[26] Proof of work is a highly computationally intensive consensus mechanism popularised by cryptocurrencies, most famously Bitcoin.

4: Illustrative conceptual model

Figure 7: Overview of the TWP – Illustrative conceptual model for a UK CBDC



Our illustrative conceptual model for a UK CBDC forms a basis for future work.

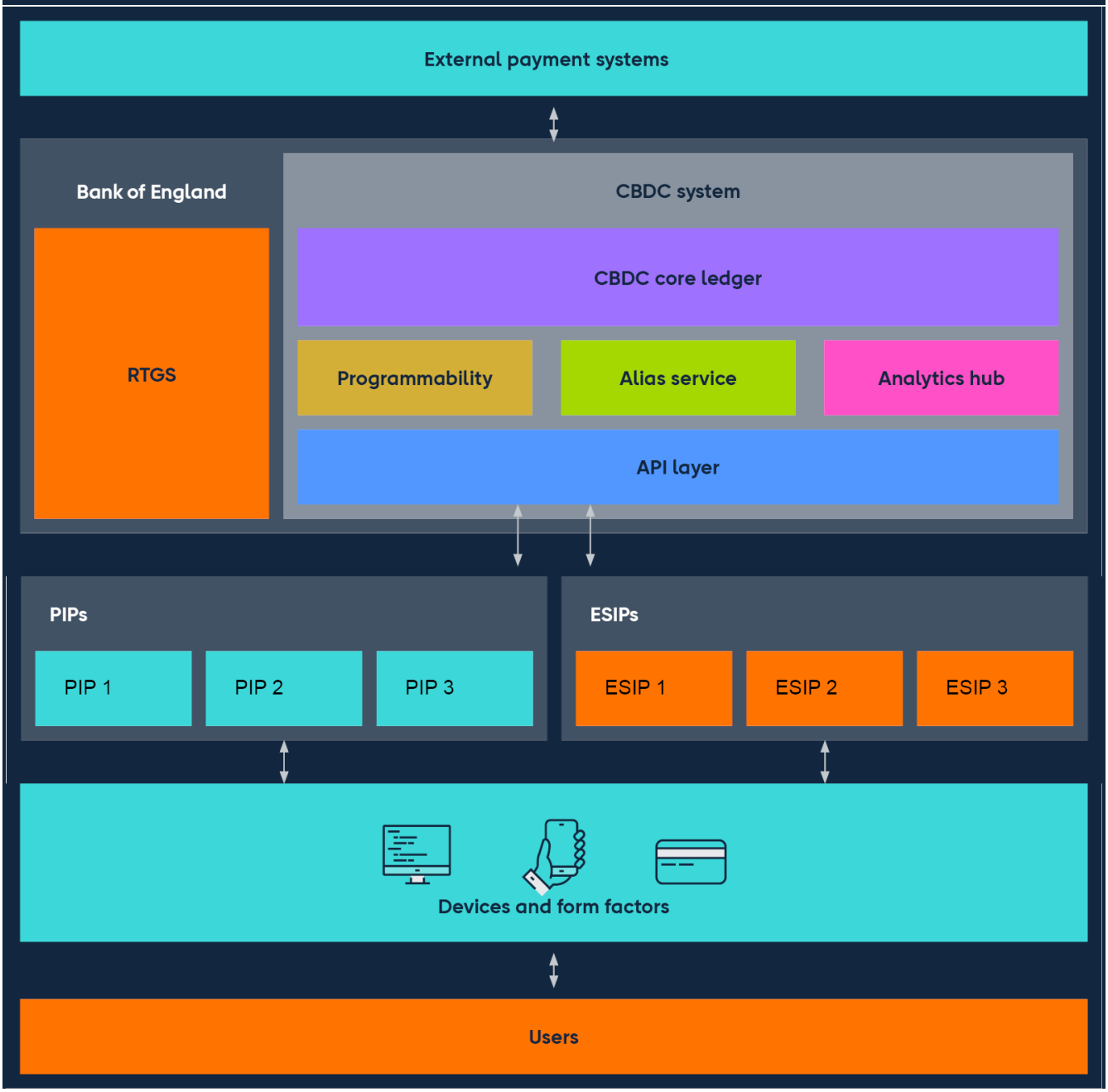
The Bank has produced an illustrative conceptual model that provides a high-level representation of a possible CBDC ecosystem, using the platform model as its basis. As discussed in the digital pound CP, the platform model comprises a core ledger and an API layer, to which PIPs and ESIPs can connect in order to provide services to CBDC users.[27]

The illustrative model set out in this paper helps to identify and examine the possible architecture, solutions and critical components that might be required for a viable CBDC system.

The illustrative model set out in this paper is not an end-state CBDC architecture. Rather, it reflects one possible approach to the architecture for a UK CBDC. There are a number of viable approaches for a UK CBDC which will be evaluated during the design phase.

[27] See Section D.1 of the **digital pound Consultation Paper**.

Figure 8: Illustrative conceptual model for a UK CBDC



There would be a range of different actors and activities in the CBDC ecosystem. Standards would be needed to define and manage their interactions and dependencies.

A CBDC ecosystem would include different actors and activities. Some activities and components would be operated by the Bank, while others would be operated by third parties. The interactions and dependencies between these components and activities would require the development of scheme rules, as well as operating and technical standards.

Table F outlines the different components and activities in a CBDC ecosystem and the actors that might be responible for building, operating and maintaining them.

Table F: Components and activities in the CBDC ecosystem

Component and Activities	Description	Responsibility
Core ledger	The central record of CBDC that records the movements of money.	Bank
Analytics	The collection and analysis of operational metadata as well as aggregated data which have been effectively anonymised.	Bank
Alias service	Aliases could be used to allow wallets to be compatible and interoperable with other payment infrastructure. For example, a long ‘card number’ for point-of-sale payments or a sort code and account number for account-to-account payments.	Bank
API layer	This would allow PIPs and ESIPs to access the core CBDC infrastructure offered by the Bank.	Bank
Programmability	The ability to run units of functionality (programs) that can effect a change on the core ledger, and can be triggered when predetermined conditions are met or initiated directly. The Bank could enable locking mechanisms that allow PIPs and ESIPs to implement certain programmability features, including smart contracts, by earmarking funds on the core ledger.	Bank (locking mechanism) Ecosystem (advanced programmable use cases and user consent)
RTGS	Existing infrastructure that holds accounts for banks, building societies and other institutions. The balances in these accounts can be used to move money in real time between these account holders; delivering final and risk-free settlement.	Bank
PIPs	These entities would have API access to the core ledger. They would provide wallet services, which would allow retail users to make payments.	Ecosystem
ESIPs	ESIPs might provide non-payment, value-add services, such as business analytics, fraud monitoring, digital identity or smart contracts.	Ecosystem
Devices	Devices that a user can use to make payments or manage their CBDC balances.	Ecosystem

4.1: Core ledger

Summary

- The CBDC core ledger would record the state information of CBDC in issue and the movement of funds.
- The core ledger would need to meet important requirements around throughput, speed, scalability, availability and privacy. These requirements would determine the choice of ledger technology.
- The use of centrally governed, distributed database technologies might be a more efficient and appropriate approach than the use of DLT solutions. However, the Bank will continue to assess a range of different approaches and will closely monitor ongoing developments in ledger technology.

The CBDC core ledger would record the state information of CBDC in issue and the movement of funds.

A ledger is a master record of chronological information for a specific type of event. For example, the debit or credit of an account linked to assets, liabilities and cashflows. Or, in token-based systems, a ledger records updates to the state and ownership of tokens or the destruction and creation of unique tokens.

Regardless of whether an account-based or a token-based approach is used for a UK CBDC, the core ledger would require a history of transactions for dispute resolution, auditing and compliance. Therefore, any UK CBDC ledger would need to record and maintain information relating to the state of the CBDC system, and the total amount of CBDC issued.

The core ledger would need to be capable of handling a large volume of transactions at high speed.

As discussed in Section 3.4, the core ledger would need to process a high number of transactions with very low latency. In order to meet these performance targets, it might be necessary to use distributed processing. This could include apportioning an even distribution of transactions across multiple machines to process in parallel; spreading the workload and minimising the potential for any processing bottlenecks. This sort of division of labour across multiple machines is an approach common to both centrally governed distributed databases as well as DLTs.

The core ledger would need to be able to scale to accommodate volumes which will fluctuate during the day, seasonally and during times of shocks.

The CBDC system would need to be able to scale elastically to make cost and energy-efficient use of the underlying ledger infrastructure. It should be automatically able to add resources to accommodate spikes in transactions due to shock events or seasonal patterns

of spending, and remove resources when transaction volumes subside. This is known as horizontal scaling.

The core ledger must achieve very high levels of availability.

Potential requirements for availability are discussed in Section 3.3, including the need for close to zero downtime. To this end, the ledger would need to be able to withstand any potential failure or outage within the platform, and self-heal.

A secondary benefit of distributed processing is that the corresponding data repositories can also be distributed. Distributing data repositories can improve the resilience of a system, particularly when updates are replicated to other participating nodes in the network.

Transaction co-ordinators might help to meet performance and resilience targets.

Transaction co-ordinators are services which play a critical role in delivering transaction-processing capabilities in distributed databases. They co-ordinate communications across processing nodes to prepare them for receiving transaction data and maintaining communication as they progress through to an atomic commitment.[28] Transaction co-ordinators also guarantee that a consensus is reached across the system.

While operating a ledger across a distributed architecture increases the potential points of hardware, software and network-related failure, it also provides contingency, as transactions can be reallocated by the transaction co-ordinator to other unaffected resources. Any transactions that may otherwise be left in an inconsistent state can be aborted, rolled back and retried, while the replication of data across many repositories mitigates against data loss as duplicate copies of state information persist in multiple locations at any one time.

A transaction co-ordinator is likely to be one of the most important elements of the ledger design. It would need to be fast, resilient, and incorporate protocols to support atomicity, consistency, isolation, and durability (ACID) properties. The most common atomic commitment protocol is two-phase commit (2PC), found in centralised distributed databases as well as some DLT solutions. The 2PC protocol ensures that when a transaction is executed, one of two outcomes is guaranteed. A transaction either completes in its entirety, or not at all, making it compliant with the ACID principles.

The CBDC core ledger must have strong security and privacy capabilities.

As discussed in Section 3.1, privacy considerations will be vital to protect users' personal data. To help achieve our technology requirements for privacy, the CBDC ledger might need to incorporate a range of privacy-enhancing techniques and policy-based access controls to ensure that data on the ledger are secure from unauthorised use.

[28] Atomic commitment occurs when a set of changes are applied as a single operation. There is no atomic commitment unless all changes are applied; if one change fails, the others are reversed.

The ledger would need to guarantee consistency across all data repositories.

Regardless of whether it uses a centralised or decentralised ledger, the CBDC system would need to guarantee consistency across all repositories of data. However, systems that prioritise the maintenance of consistency across instances usually do so at the expense of high transaction throughput. Conversely, systems that prioritise fast transaction processing often do so at the expense of consistency.

This poses a challenge for CBDC, as a solution must be capable of settling transactions quickly, while providing low-latency retrieval of the current-state information recorded in the ledger.

DLT and blockchain-based solutions have relevant features for a CBDC core ledger, but they would also face familiar engineering challenges.

In a permissionless, low-trust model, state information is replicated and maintained across multiple instances of a data repository. Each instance of a repository would represent a copy of the ledger in its entirety and could be hosted by many different participating entities in the network.

A transaction co-ordinator in this model would be responsible for broadcasting updates to all data repositories and co-ordinating responses to ensure that a consensus has been achieved. In theory, this model would be highly resilient, but it presents privacy and scalability challenges that might limit its ability to meet requirements for a CBDC.

Alternatively, in a permissioned DLT model, access to data can be restricted so that state information is partitioned across a group of permissioned entities and no single entity possesses the ledger in its entirety. In this approach, PIPs might maintain their own localised data repositories, representing their individual slice of the system's state (ie information relating only to the transactions that they have initiated or received).

The Bank's role in this model would be to operate a service on the network that facilitates the safe execution of transactions by validating their authenticity. This service is often referred to as a central bank's 'notary node'.

In this model a transaction co-ordinator and consensus protocol combine to co-ordinate communication between transacting parties and the central bank's notary node(s). As updates do not need to propagate to all data repositories in a network, the amount of information broadcast would be reduced dramatically. However, it would still be challenging to achieve very fast transaction processing given that the central bank's notary would likely be a bottleneck on that network, as well as a single point of failure.

Despite these developments in alternative architectures and data technologies, significant engineering challenges remain. The 'Blockchain Trilemma'[29] theory posits that it is extremely difficult for any blockchain protocol to achieve three crucial system guarantees simultaneously: decentralised, scalable and secure. Federating the responsibility for processing transactions across a distributed ledger may increase resilience, but achieving the necessary transaction throughput remains challenging.

There is continuing effort to address some of the scaling challenges in DLT, such as 'layer 2' solutions that localise transaction processing to speed up throughput. But these solutions could impose architecture design choices that might be suboptimal and which have unintended consequences elsewhere across the CBDC system.

A number of features of DLT may not be applicable to, or necessary for, a CBDC use case.

DLT approaches might impose undesirable decentralisation of other aspects of a system, such as governance or administration. DLT features that support information exchange in a trustless network may not be necessary for a CBDC use case. These features might also introduce unnecessary technical complexity. Further, it may also be possible to achieve some of the benefits of DLT, such as resilience, redundancy and security, via alternative and well-established data management strategies, using distributed, centrally managed databases.

A white paper from the UK's National Cyber Security Centre (NCSC)[30] concluded that DLT is only likely to be useful in circumstances where all the following statements are true:

a) Multiple entities need to be able to write data.

b) There is a lack of trust between the entities writing data.

c) There is no trusted central authority that can write data on behalf of the entities.

If any one of the above statements is assessed to be false, then the NCSC considers that a 'conventional technology, like a database, is likely to be more appropriate'.

Based on the Bank's current thinking on requirements for the core ledger, the use of centrally governed, distributed database technologies, might be a more efficient and appropriate approach than the use of DLT solutions. However, the Bank will continue to assess a range of approaches, and continue to monitor ongoing technology developments.

[29] **The Washington Post (2022) – The 'Blockchain Trilemma' That's Holding Crypto Back**. **Why sharding is great: demystifying the technical properties**.
[30] **NCSC (2021) – Distributed ledger technology**.

Next steps

The Bank will assess requirements for operating a CBDC ledger at scale and will conduct practical experimentation to test different architectural approaches and ledger structures. That research will also determine any technology trade-offs related to ledger design.

The Bank will conduct data modelling to understand the structure of the information on the ledger that is necessary to capture the state of the CBDC system.

The Bank will also assess the state of modern in-memory transactional databases.

4.2: Analytics

Summary

- The Bank may need to collect operational data for the purpose of maintaining and operating a stable, secure and efficient CBDC system.
- Data should be collected and analysed on a separate platform dedicated to supporting analytics.
- The Bank would not collect or analyse users' personal data.

In performing the functions of operating, maintaining, and securing the core ledger and API layer, the Bank would need to collect operational metadata for predictive, real-time and historical aggregate analysis of system status and performance.

The analysis of operational metadata supports the stability and efficiency of the Bank-provided core ledger and API layer. Therefore, an engineered data pipeline could collect the relevant data from both the core ledger and the API layer, transforming these data in flight, and persisting to a platform where analysis can be undertaken safely, away from the core systems. This data platform could be configured specifically for data analytics, reporting and modelling. It would also be used to pre-empt and alert system failures, bottlenecks and anomalous events that may negatively impact the performance and efficiency of the CBDC system.

Much as it does today with existing payment infrastructure, the Bank may also wish to collect aggregate data, which have been effectively anonymised, for the purposes of economic and policy analysis, in the course of its duties for monetary and financial stability.

Importantly, no CBDC user would be identifiable through the analysis of these data. The Bank will consult in due course on what aggregated data might be collected and for what purposes.

Next steps

The Bank will assess different options available for enabling appropriate data analytics and determine the analytical workloads necessary to support operation of the CBDC system.

4.3: Alias service

Summary

- To interoperate with existing payments infrastructures and enhance CBDC functionality, wallets could have aliases.
- To allow for greater flexibility, aliases could be either well known (rarely changed) or disposable (frequently changed).
- Some examples of commonly used aliases are phone numbers, sort code and account numbers, card numbers (primary account number (PAN)) and wallet IDs.

CBDC wallets could use aliases in order to facilitate interoperability with existing payment infrastructures.

As discussed in the digital pound CP, a UK CBDC would initially focus on in-store, online and P2P payments.[31] It would also enable interoperability with other forms of money, particularly cash and bank deposits. No decision has yet been made on the format of wallet addresses or CBDC wallet identifiers. But a CBDC wallet might use aliases in order to interoperate with the range of existing payment infrastructures. An example of a widely used alias is a debit card, which can act as the alias of a bank current account. The use of aliases could support interoperability with other payment infrastructure, such as point-of-sale (PoS) hardware and account-to-account systems. It might also allow payments via alternative identifiers, such as a phone number, etc (subject to fulfilling necessary legal, regulatory and security obligations).

In this paper, the alias service is shown as part of the Bank-managed infrastructure. This is primarily to allow the routing of message requests between PIPs and to reduce alias collision. However, it may be possible to distribute this functionality across the ecosystem.

The alias service would be designed to ensure privacy and user control of personal data.

The alias service would be designed to ensure privacy, in line with the Bank and HM Treasury's objectives for CBDC. One way to ensure that the alias service would not access personal information could be to only store a one-way hash of the alias. The hash value would then be used by PIPs to look up the wallet and PIP responsible for that wallet in order to make the subsequent payment.

Privacy is an essential feature for users, but there are times when users may not wish to be private, for example when paying friends and family. Users may also want to allow trusted

[31] See Section D.3 of the **digital pound Consultation Paper**.

people to save their wallet details so they can be paid again in the future. PIPs, rather than the Bank, would be responsible for implementing user-privacy preferences of this sort.

To meet these requirements, a CBDC might have both a well-known and a disposable alias.

A well-known alias changes rarely and is something the wallet holder is happy to be shared with, and stored by, third parties. For example, users may choose to link their mobile phone numbers to their wallets so that a messaging service might use their phone numbers to facilitate CBDC payments.

A disposable alias, as the name suggests, is used for a short period of time. It is useful where a user wants to be able to conduct a transaction in private and not allow the recipient a record of their identity. For example, when buying groceries or coffee, users may elect to use a disposable alias. Disposable aliases would constantly change, so they may need to be recycled or archived after an appropriate amount of time to reduce the volume of information stored in the alias service. As increased volume could slow the performance of the alias service, managing the scaling and recycling of aliases would be critical.

A wallet holder might have both well-known and disposable aliases on their wallet at the same time. They should always have at least one alias so that the core wallet identifier is never exposed. This ensures there is always a level of abstraction and protection of the core wallet identifier, protecting it from being compromised. If an alias were to be compromised, a new alias can be created rather than having to create a new wallet.

The initial design for aliases could include:

- Phone number: These aliases might enable fast payments to and from mobile phone numbers. These aliases are unlikely to be disposable.
- PAN alias: Primary account number (PAN) is the technical name for the long number on a debit or credit card. These aliases would enable payment at PoS terminals.
- Account number and sort code: These aliases would follow the same standard as UK current accounts and would be used to enable payments to and from bank accounts.
- Wallet alias: These aliases would be used for CBDC-to-CBDC payments.

Aliases must be compatible with PIPs' obligations to comply with KYC and AML regulations.

While a user may choose to use a disposable alias for a specific payment, their own wallet provider would still know who they are. The alias design allows privacy for the payer from the payee and vice versa, but not privacy from their PIPs. PIPs must still be able to fulfil their regulatory obligations around AML and KYC.

Next steps

The Bank will investigate how to support the necessary types of aliases to ensure that the CBDC system has flexibility and privacy.

The Bank will also conduct further research into whether the alias service can be decentralised without impacting performance and increasing alias contention.

4.4: API layer

Summary

- The API layer allows external parties (PIPs and ESIPs) to access the core CBDC infrastructure offered by the Bank.
- The API layer aims to be use case agnostic, allowing external parties to build a diverse range of innovative services for the end user.
- The API layer architecture should be designed with a strong focus on usability, security and the ability to introduce new innovative functionality without compromising core use cases.
- The Bank is experimenting with API design through Project Rosalind in conjunction with the BIS Innovation Hub London Centre.

The API layer would allow PIPs and ESIPs to build overlay services.

The core ledger would provide the minimum necessary functionality for managing a CBDC wallet and making payments using CBDC. The API layer would allow PIPs and ESIPs to access this functionality, allowing them to build overlay services that make CBDC usable and useful.

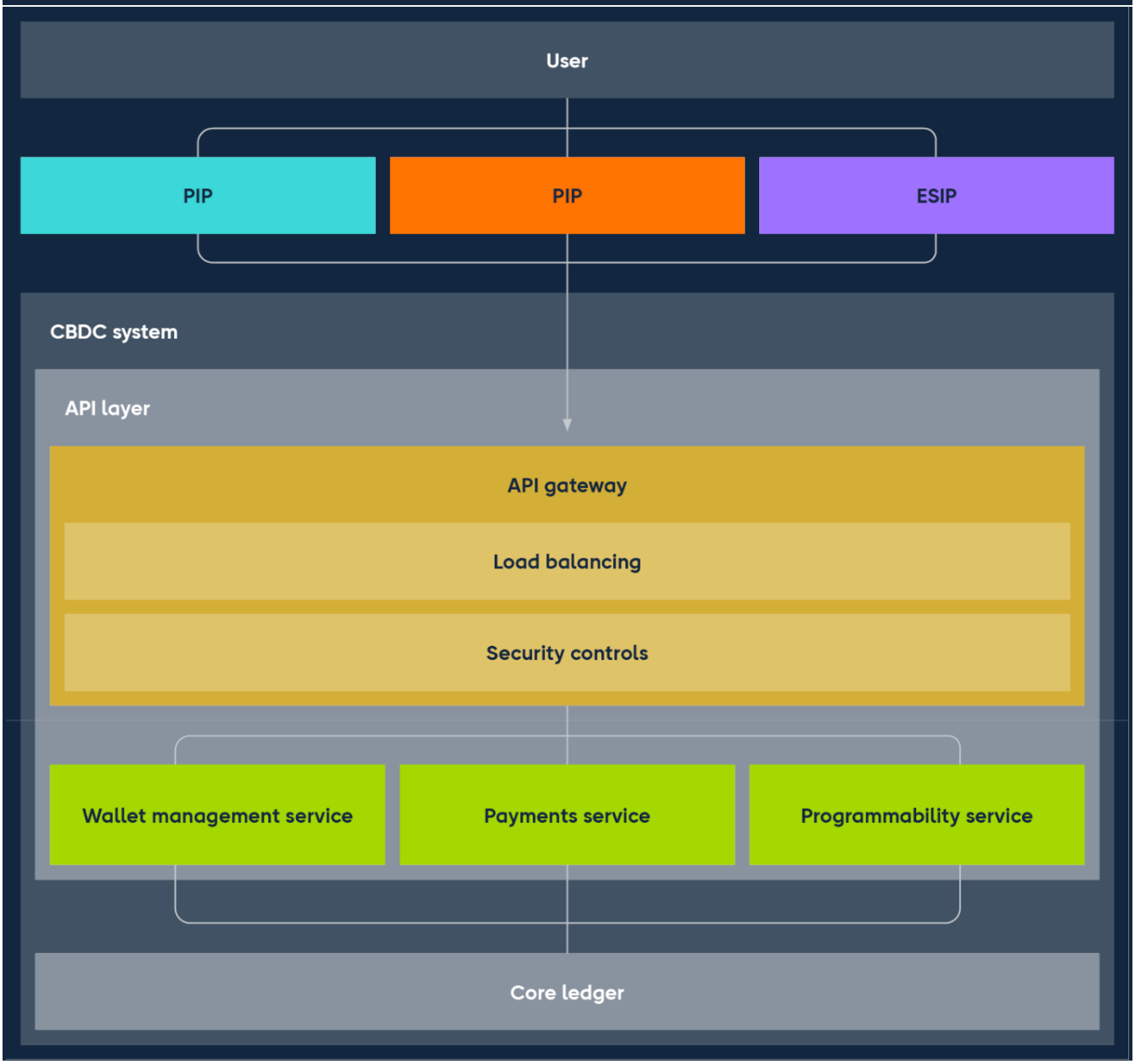
A well-designed API layer would allow PIPs to integrate their current and future payment services with a CBDC. The API layer should also be designed with the aim of encouraging a range of innovative digital products and services that add value for users.

The API layer would facilitate instructions and data sharing between PIPs, ESIPs and the core ledger, in a secure and efficient way.

A potential API architecture would consist of two key components, an API gateway and API services:

- The API gateway would provide a single entry point for API calls, which enables efficient and secure management of the API requests by routing valid requests to the appropriate service.
- The API services would implement the different core functionality accessed through the API layer.

Figure 9: The API layer



Security standards should be built into the API layer.

API authentication and authorisation methods would need to be complemented with security controls that prevent distributed denial of service (DDoS) attacks. Authentication involves verifying the credentials of the parties involved, while authorisation involves identifying the services a given PIP or ESIP has access to. Open standards like Open ID[32] and OAuth[33] might be used to implement authentication and authorisation functionality in a standardised

[32] Open ID is an open authentication protocol. It enables end-users to be authenticated using single-sign-on.
[33] OAuth is an open standard for granting access to a system's services.

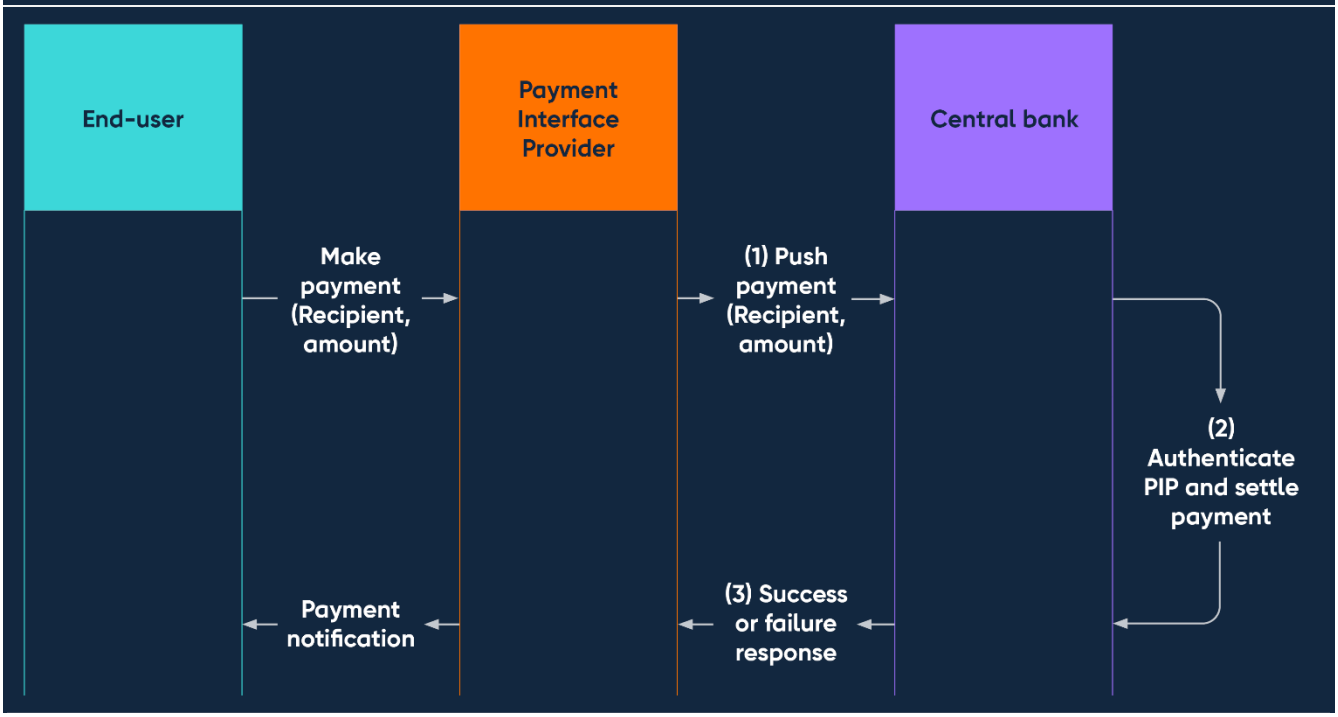
manner.[34] In addition more rigorous controls like the Financial-grade API standard[35] would be considered to ensure the highest standards of security controls are in place.

The API specification could standardise CBDC data and instructions exchange by providing a common definition of the functionality and expected behaviour of the API.

The API layer could orchestrate CBDC payment flows as displayed in Figure 10. At a minimum the API might:

- identify a request from an authorised PIP or ESIP (eg a user that wants to initiate a payment through a wallet provided by a PIP);
- send the request to a given service that would implement the request (eg calculate the sender's account balance and settle the payment); and
- finally, report the retrieved information back to the user through the wallet (eg the money has been sent and the new balance will be displayed).

Figure 10: CBDC payment flow orchestration



[34] Separately, in relation to the RTGS Renewal Programme, the Bank is working closely with payments industry experts on a draft framework for the domestic harmonisation of API technical standards and will consult on a proposal soon. We will ensure that, if and where appropriate, the CBDC APIs are aligned with this framework.
[35] Financial-grade API is a security framework developed by the Open ID Foundation providing technical guidance for securely using APIs that utilise financial data.

The API specification should be designed to enable access and adoption by PIPs and ESIPs.

To the maximum extent possible, the API should be agnostic to the core ledger technology. For instance, whether monetary units are token or account based, or whether the core ledger is centralised or distributed.

Other design considerations for the API layer are:

- The API should be use case agnostic; a core set of API functions should support a large number of use cases.
- The API specification must be designed with simplicity at its core, enabling easy integration for PIP and ESIP internal systems.
- The API should be well documented to enable adoption.
- The API specification should be stable and should not require frequent updates.
- The API layer should be reliable. Multiple identical requests should always receive the same response, error messages should be clear and concise.
- The API specification should consist of a number of well-defined functions, to support extensibility (see Section 3.5). Highly encapsulated API specifications could facilitate a higher degree of extensibility and legacy compatibility during upgrades.
- The governance of the API layer should be clearly defined from the beginning to ensure minimal impact in the CBDC ecosystem when changes are implemented in the API layer.

Box A: Project Rosalind

Project Rosalind is a collaboration between the BIS Innovation Hub London Centre and the Bank. The project aims to develop a best-in-class API specification for a retail CBDC in order to gain understanding on how a CBDC could deliver its core functionality. By focusing on the API design, Rosalind allows the design of the core ledger to be abstracted.

The project will explore some of the functionalities required to enable a diverse and innovative set of use cases developed by the private sector. Through this experimentation, the project aims to study how best to define a robust API layer which could lay the foundation for a successful CBDC ecosystem.

Further information on Project Rosalind can be found on the **BIS website**.

Next steps

The Bank will continue to participate in Project Rosalind to develop a best-in-class retail CBDC API and assess its usability when opened up for experimentation.

The Bank will incorporate the lessons learned from Project Rosalind into the design of the API layer for the UK CBDC.

4.5: Devices and payments

Summary

- To achieve its objective as a monetary anchor, CBDC must be widely available and usable.
- Technical standards for payments between devices would be needed to ensure interoperability and minimum standards of security and functionality.
- CBDC would be available to users via a wallet, as well as via physical smart cards. It should enable online, in-store and peer-to-peer payments.

Technical standards are needed to ensure that CBDC wallets are interoperable, offer a consistent minimum level of functionality, and are secure.

Users should be able to make and receive payments using a range of devices and form factors, including (but not exclusively):

- Smart devices
- Smart cards
- E-commerce websites and applications
- PoS devices

While these devices and form factors would be developed by third parties, the Bank would define aspects of how they operate. This would ensure interoperability, deliver a common minimum level of functionality, ensure security and preserve the open nature of the CBDC system.

Users should be able to access CBDC via smart devices, including smartphones.

Smartphones have become central to people's financial lives with the introduction of mobile banking apps and wallets. In order to support adoption, a CBDC system should allow PIPs to develop smartphone-based CBDC wallets, offering in-store, peer-to-peer and e-commerce payments. To further encourage innovation, users might also be able to access their wallets using wearables and smart IoT devices.

Users should also be able to access CBDC without a smart device, for example via smart cards.

CBDC should also be accessible via smart cards to support users who do not have a smartphone. Smart cards are plastic cards with an integrated circuit chip, similar to credit or debit cards. There are certain circumstances that may present challenges for smart card payments. For example, where both the payer and the payee are using smart cards, a challenge arises since the cards would require a power source, as well as a way for the user

to define the transaction value. While smart cards which contain batteries, screens, keypads and even fingerprint scanners do exist, they are more costly to issue.

CBDC should support e-commerce transactions.

E-commerce transactions take a variety of forms, including web pages on mobile and desktop browsers, and in-app payments on smart phones, games consoles and a growing range of devices. The API layer should enable wallet providers to support payments across the range of e-commerce methods and devices either through integrating CBDC payments into existing checkout pages or by creating custom CBDC payment flows.

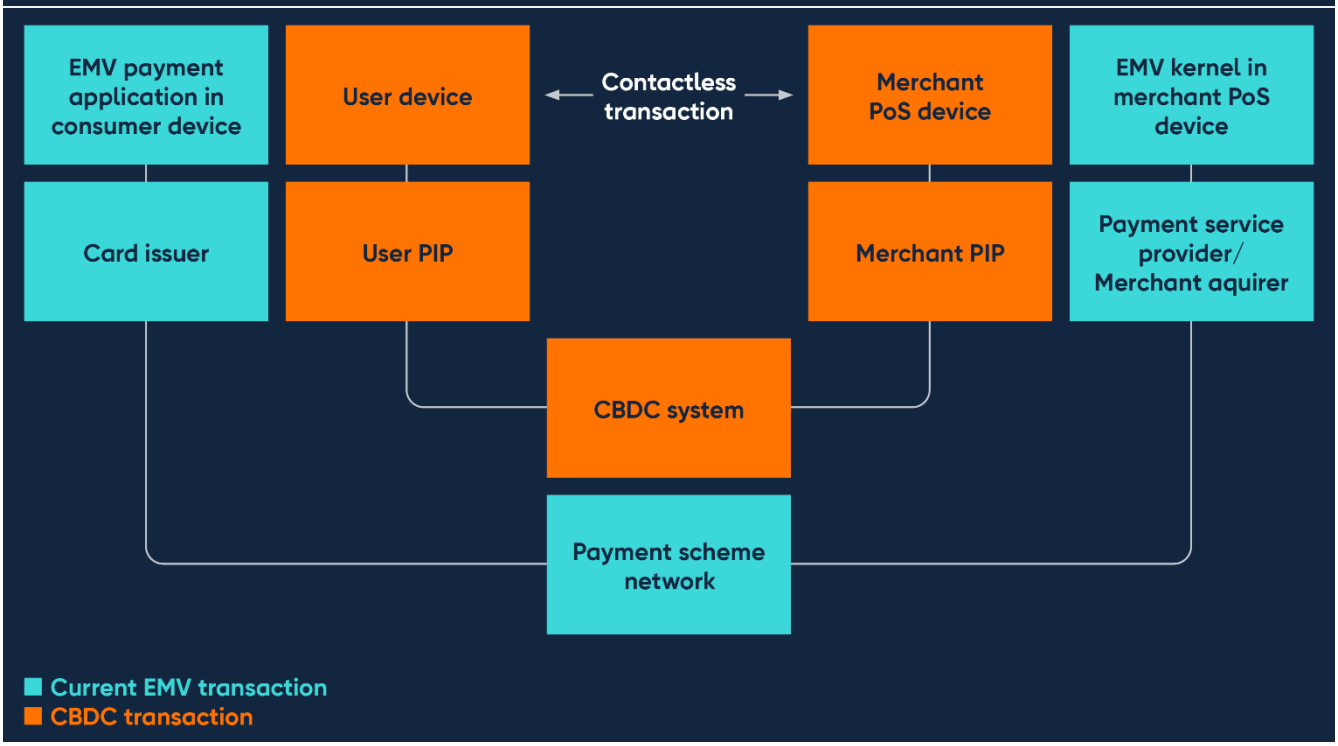
For CBDC to be useful for everyday payments, users would need to be able to pay in store for purchases.

To ensure utility and support adoption, CBDC would need to be widely accepted in stores. Therefore, it is likely that the CBDC system would be designed to allow merchants to use existing PoS terminals to accept CBDC payments. This would eliminate the need for merchants to invest in new hardware. Existing PoS technology also has the advantage of familiarity for merchants as well as wide hardware coverage.

The Bank commissioned a feasibility study which explored how CBDC could be accepted for payments using the existing PoS estate in the UK. The study concluded that it would be feasible to use existing PoS infrastructure to accept CBDC payments, and that there are several viable ways of doing so. The study also highlighted that there are parallels between an existing EMV[36] contactless transaction and a CBDC transaction, as shown in Figure 11.

[36] EMV is a set of specifications which enable smart card-based payments to be consistently accepted across different payment schemes.

Figure 11: Parallels between EMV contactless transactions and CBDC transactions



The study concluded that there are four key design questions to be answered in order to enable CBDC payments at PoS:

- Would the user's payment device be 'balance aware'?
- Which contactless kernel might CBDC use?
- How would users be authenticated?
- Which transaction flow might CBDC payments use?

Would the user's payment device be 'balance aware'?

A user's balance could either be stored on their device or remotely on the ledger.

The location where the balance is stored determines how payments are processed. Debit and credit cards store balances remotely with the issuing entity; the card number is used as a look up to check the balance at the issuer. Storing balances remotely on the ledger should be feasible since most in-store payments currently use a connected terminal, which would enable connectivity with the ledger. This approach would also reduce the impact of a user losing their device, as it would not result in the user losing their CBDC funds.

Offline payments may require that balances be stored on user devices. This could pose challenges for e-commerce payments.

Storing balances remotely on the core ledger creates challenges for offline payments since no look-up to the ledger is possible due to a lack of connectivity. In order for payments to work without internet connectivity, the device would need to be aware of the user's balance so that they do not spend money that they do not have.

However, for e-commerce payments, the user's balance must also be able to be sent to recipient website or application. If a user's balance were held directly on their device, rather than remotely, the device would need to take part in any e-commerce transaction to transfer the balance to the recipient website or application. This requires the device to have internet connectivity, which may be challenging for smart cards. Similarly, if a payment failed due to technical issues with the website, application or connectivity, the user's balance would have to be restored to the device, which could also prove challenging.

A combination of on-device and remote ledger storage might be needed.

In the platform model, user balances are stored remotely on the core ledger. But it might be possible to use a hybrid approach, where users are able to download some of their balance to their devices to support offline transactions. However, this fragmentation of a user's balance might pose challenges for user experience.

Which contactless kernel might CBDC use?

In order to support CBDC payments using existing infrastructure, PoS devices will require a contactless kernel.

A kernel is a piece of self-contained software which provides payment acceptance devices with the necessary functions to process contactless transactions. There are several different contactless kernels in use today for different scenarios and payment networks.

The feasibility study highlighted four possible options for kernels to initiate CBDC payments at PoS:

- Develop a bespoke CBDC contactless kernel.
- License a 'white label' kernel from an existing vendor.
- Use an implementation of the proposed EMV Contactless Kernel Specification known as 'Kernel 8'.
- License an existing payment network's kernel.

How might users be authenticated?

Users would need to be authenticated to carry out CBDC transactions.

PIPs would be responsible for authenticating users. This is the Bank's preferred approach to user authentication as it allocates the responsibility for onboarding, AML and KYC checks to PIPs, and does not require the Bank to store personal data. PIPs would likely need to comply with strong customer authentication (SCA) requirements.[37] This means that users might have to authenticate two or more elements categorised as:

- knowledge (something you know) – A personal identification number (PIN) or password validated either locally on the device or online;

[37] **Payment Services Regulations 2017, Regulation 100**; **Payment Services Directive ((EU) 2015/2366) (PSD2), Articles 4 and 97**.

- possession (something you have) – In most cases, this would be either the smart device or the smart card; and
- inherence (something you are) – Biometric authentication, such as facial or fingerprint recognition.

If CBDC were to be based upon EMV contactless standards, there are a number of different verification methods available. These include:

- Offline PIN (chip and pin) – where the PIN is verified offline by the chip on the user's smart card.
- Online PIN – where the PIN is encrypted by the terminal and sent to the card issuer for verification. In CBDC, this verification could be done by the user's PIP.
- Consumer Device Customer Verification Method (CDCVM) – where the card or device verifies the user, then sends a signed message to the issuer that the user has been authenticated. Examples include fingerprint or facial recognition on smart phones, and entering PINs into smart cards or devices.

Online PIN and CDCVM are likely to be most relevant for CBDC.

Offline PIN would not work for smart devices, as it requires that a card with a chip be inserted into the PoS terminal. Offline PIN also requires a different kernel compared to contactless, so it would further complicate the development and deployment of CBDC payments. Therefore, the most likely verification methods for CBDC would be Online PIN and CDCVM.

Which transaction flow might CBDC payments use?

There are several possible flows for CBDC payments at PoS. At a high level, the options are:

a) If the balance is stored on the ledger:
   - PULL – A request (to transfer funds from the user to the merchant) is sent from the merchant's PIP to the core ledger. As the instruction is coming from the merchant PIP, rather than the users PIP, the ledger would need to be able to confirm that it reflects a valid instruction from the user.
   - PUSH – A request (to transfer funds from the user to the merchant) is initially sent from the merchant's PIP to the consumer's PIP. This request might either be passed via the core ledger API, or via direct communication between PIPs. If the user's PIP successfully authenticates the request, it then sends an instruction to the core ledger, to transfer funds from the user to the merchant.

b) If the balance is stored on devices:
   - PEER/OFFLINE – The user's device directly transfers the balance to the merchant's wallet. The core ledger is updated later with details the transfer.

A PUSH flow is likely to be more suitable than a PULL flow, as it does not require the core ledger to validate users or devices. PEER/OFFLINE may also be relevant for enabling offline peer-to-peer payments. The Bank will continue research and experimentation to determine which of these transaction flows would be most appropriate for a CBDC.

Next steps

The Bank will continue to experiment with different options and solutions that may help to support the delivery of an innovative and user-friendly CBDC payments experience.

4.6: Interoperability

Summary

- A CBDC should be interoperable with other forms of money, particularly cash and bank deposits.
- If interoperability between a CBDC, cash and bank deposits can be delivered effectively through existing payments infrastructure, then that is likely to be the preferred option. However, it will also be necessary to evaluate whether new or additional infrastructures would be required.
- Interoperability will be a priority area for research and experimentation during the design phase, including through collaboration with the financial sector, technologists and other central banks.

As outlined in the digital pound CP, a UK CBDC should enable interoperability with other forms of money, particularly between:

- **CBDC and bank deposits:** to enable users to convert into and out of bank deposits, and make and receive payments between CBDC wallets and bank accounts.
- **CBDC and cash:** to enable users to convert into and out of cash. Given the physical nature of cash, this would need physical infrastructure as well as technology solutions.

Interoperating with bank deposits

Using existing payments infrastructure to enable interoperability with bank deposits is likely to be the most effective and efficient route; subject to technical, functional and operational viability. The Bank will conduct further research and evaluation to determine whether existing infrastructures can deliver the necessary functionality for interoperability, or whether new or additional infrastructures are needed.

In particular, one option could be to use account-to-account payment infrastructure, such as Faster Payment System (FPS) or the New Payments Architecture. Additional integrations might be added later to support specific use cases. For example, Bacs might be added to support wage payments and another integration might be added if end-of-day sweeping is required for merchant accounts. Any such integrations would require further analysis to examine the feasibility and implications of implementing them.

In order to integrate with existing payment infrastructure, CBDC wallets might use an account number and sort code alias. The Bank will assess, with relevant stakeholders, the viability and desirability of such approaches, including, where appropriate, possible proofs of concept or feasibility tests.

Interoperability with cash

Existing infrastructure might also be used to enable interoperability with cash. This points towards exploring the feasibility of using infrastructures, such as LINK, for CBDC to cash conversions.

Since ATMs are predominantly cash dispensing (while it is an option to have them accept cash deposits it is not the dominant mode), the Bank will conduct further investigation into whether cash to CBDC conversion could be automated. However, for reasons of practicality and financial inclusion, some level of ‘in-person’ service is likely to be needed. This will be subject to further exploration.

Next steps

The Bank will engage with stakeholders to determine the functionality necessary for enabling conversions between CBDC and other forms of money, including, where appropriate, possible proofs of concept or feasibility tests.

Interoperability will be a priority area for research and experimentation during the design phase, including through collaboration with the financial sector, technologists and other central banks.

4.7: Programmability

Summary

- The Bank will not implement central bank-initiated programmable functions. Instead, the Bank would provide the necessary infrastructure for the private sector to implement programmability features for users. Those features would require user consent.
- Programmable functions should not reduce the simplicity and performance of the core ledger, so smart contracts would not be hosted on the core ledger.
- The Bank's initial exploration of programmability focuses on enabling a range of programmable features through API access to a simple locking mechanism on the core ledger.

The Bank will not develop or implement central bank-initiated programmable functions.

Central bank-initiated programmable use cases are not currently relevant to the Bank and HM Treasury's policy objectives for CBDC. Further, this functionality could damage the uniformity of the CBDC and cause user distrust. For these reasons, the Bank will not pursue central bank-initiated programmable functions.

However, during our research, stakeholders highlighted the benefits of programmability for innovation and user experience. As such, the Bank would aim to support programmable functionality and use cases which are designed to give users greater functionality from their wallets and CBDC holdings. These functionalities would be implemented by PIPs and ESIPs, and would require user consent. PIPs could implement some of these features, such as automated payments and programmable wallets, by hosting the programmable logic, and updating the core ledger with the result via the API. But other features, such as payment-versus-payment (PvP), delivery-versus-payment (DvP) and smart contracts, might require additional design considerations. In those instances, the Bank would only provide the necessary infrastructure to support PIPs and ESIPs to provide these functionalities.

Table G: Programmable features and their priority

Programmable features	Priority
Central bank-initiated programmable functions	Will not enable
Automated payments	Desirable
Programmable wallets	Desirable
Payment-versus-payment	Requires further assessment
Delivery-versus-payment	Requires further assessment
Smart contracts	Requires further assessment

Automated payments

An automated payment refers to any machine-initiated payment that is not reliant on human interaction. These payments are often triggered by simple conditions, such as the date and time when a payment should be made. For example: ‘on the last day of each month, make a payment of £Y to X’. This matches the logic behind standing orders and recurring payments. The functionality for time-based payments is commonplace for users today and can be programmed by users relatively easily.

An automated payment could be particularly useful in IoT use cases, where machine-to-machine payments are enabled. Although this may require more complex logic to be stored and executed by a PIP or ESIP, it might still be achievable via simple API access to the core ledger and an internet connection.

Indicative automated payments use cases:

- Creating a standing order to pay a charity once per month in CBDC.
- An automated payment made by a vehicle at a toll booth.
- A parent automating an allowance to be sent to their child every Monday.
- A digital marketplace automating the payment to the manufacturer and delivery company when a sale is made.

Automated payments might be enabled via API access.

Such functionality might be enabled by providing API access to PIPs. By allowing a PIP to initiate a payment via API on the core ledger, PIPs could host their own logic that triggers a payment; much like how standing orders are set up currently. A user could simply pre-program set payment conditions through an app hosted by their PIP, who would then initiate the transaction as configured by the user.

If a payment were initiated but the user does not have funds available, the payment would fail and an error response would be provided to the wallet application. PIPs might be responsible for ensuring the resolution of failed payments is handled in a consistent and fair manner.

Programmable wallets

Programmable wallets are wallets that allow some level of user configuration or additional service. They might allow users to set rules to manage their own funds.

For example, users could round up transactions into a savings pot or set rules to help them budget. Such features exist in some financial products today and would be developed by the private sector. Importantly, programmable wallets place control over the rules in the hands of the user.

Indicative programmable wallet use cases:

- Creating a savings pot to help budget or save for a larger item (eg a holiday).
- 'If This Then That' user programmability of a CBDC wallet, allowing a user to configure their wallet to implement conditional payments of their own choice.
- Budgeting tools, allowing the user to set rules for how much they spend on different goods and services.

Programmable wallets may not require API functionality and could instead be enabled entirely by PIPs.

Programmable wallets may not require additional API functionality beyond the basic configuration. For example, saving pots or budgets could be configured by users and developed entirely by PIPs, independent of the central bank or CBDC system.

PvP, DvP and smart contracts

PvP is the process by which the final transfer of a payment occurs if and only if the final transfer of another linked payment also takes place. PvP functionality might be used to enable interoperability and exchange between a CBDC and other forms of money, such as stablecoins.

DvP is the process that links an asset transfer and a funds transfer in a way that ensures that delivery occurs if, and only if, the corresponding payment occurs. Both PvP and DvP reduce settlement risk, and costs, by enabling greater automation in settlement.

A smart contract is the automation of business logic based on pre-determined terms and conditions. This concept has been popularised by permissionless blockchain technologies, such as Ethereum, but is not exclusive to any specific technology solution.

In a smart contract, the terms of a contract are specified in the form of a program which states the terms and parties involved. Funds required for the transaction to execute are earmarked, and a payment will execute only when the terms of the smart contract agreement have been met.

Smart contracts might offer innovative and, potentially, more efficient ways for processes to be orchestrated. Such functionality has a wide range of potential use cases. Even simple versions of smart contract functionality may be enough to enable PvP and DvP within the CBDC ecosystem.

Indicative PvP, DvP and smart contract use cases:

- An insurance claim governed by a smart contract, whereby a claim is instantly paid out when set conditions have been met.
- Instantaneous currency exchanges with reduced settlement risk.
- More efficient real estate purchases, whereby all parties' transactions are executed simultaneously by a smart contract.

Models for enabling smart contracts come with additional complexity and risk.

If smart contracts were hosted on the core ledger, they could become complex additions. They may introduce new technology and risk requirements, such as increased storage requirements to support smart contracts or higher performance requirements to support the additional smart contract processes. They may also introduce risk to the CBDC system. For example, the risk that a malfunctioning smart contract could harm CBDC availability or throughput. Trade-offs will be carefully considered around:

- What functionality can be performed in a smart contract?
- Who can develop a smart contract?
- How are smart contracts verified?
- What happens when a smart contract fails?

Ethereum model

Blockchains, such as Ethereum, have popularised smart contracts by allowing contracts to be hosted, orchestrated and executed on the blockchain itself via the Ethereum Virtual Machine (EVM).

The Ethereum approach would require the Bank to host and orchestrate wide-ranging business logic on behalf of others, in the form of smart contracts. Given our aim to provide the minimum necessary functionality for CBDC, this activity is best left to the private sector. Hosting business logic also creates a number of reputational risks and potential conflicts. It could also create technical challenges or inhibit the performance of the core CBDC system.

Avalanche model

Avalanche is a popular blockchain that aims to segregate the smart contract platform from the core transaction ledger. It addresses some of the performance constraints of the Ethereum model by enabling increased volume for smart contract transactions while offering many of the functionality benefits.

This architecture requires multiple ledgers to be hosted – at a minimum, one for processing transactions that exchange digital assets or payments, and one for hosting smart contracts. In the Avalanche model, the EVM is used for the smart contract platform. This enables some interoperability with Ethereum applications, code, and its community of developers.

Segregating the smart contract platform from the core ledger may be one way to address the additional performance demands while ensuring that simple payments are always fast and available, but this would require us to host a smart contract platform and would expose the Bank to operational risks and other considerations highlighted above.

> **Smart contract architectures may not be appropriate for the core CBDC system, but some functionality might be enabled elsewhere in the ecosystem.**

To ensure that the core ledger is as simple, resilient and performant as possible, and to support private sector innovation, the Bank considers that complex business logic for smart contracts should not be hosted on the CBDC ledger. This means that the Ethereum and Avalanche approaches to smart contracts may not be appropriate for a UK CBDC. However, it might be possible for certain elements and functionalities of these approaches to be enabled off-ledger by PIPs and ESIPs as part of the wider CBDC ecosystem.

During the forthcoming design phase, the Bank will continue to examine solutions, together with the private sector, that enable smart contracts and interoperability with different programmable platforms. Determining whether the CBDC system can support smart contract functionality, while not compromising simplicity, resilience or performance in the core ledger will remain our guiding principle in those experimentations.

Regulatory and liability frameworks may need to be put in place.

Depending on the specific implementations and use cases determined by end-users and the private sector, smart contracts might also raise policy considerations around resilience, operational risk, consumer protection and liability for loss. This would require careful analysis before committing to enabling smart contracts functionality.

While smart contracts might offer potential benefits for users through enabling more efficient processes, the legal and regulatory framework is evolving alongside the technology. A clear liability framework would need to exist to ensure that consumers interacting with smart contract features are clear on who bears responsibility for any financial losses incurred.

A range of programmable features might be enabled by providing API access to locking mechanisms on the core ledger.

A CBDC might enable a range of features, including DvP, PvP and smart contracts, by providing API access to simple primitives, eg locking mechanisms with configurable conditions on the core ledger.

This is based on the principle that if certainty of settlement can be ensured for funds on the CBDC ledger via a locking mechanism, this enables PIPs and ESIPs to facilitate more complex programmable functionality off ledger. However, this may come at the expense of some loss of liquidity, where funds are locked pending the processing of smart contract terms.

Such a locking mechanism could require:

- earmarking funds with set conditions on when the funds can be released; and
- programming the earmarked funds to only release the payment when a linked account or event has completed their stage or conditions under the contract or programmed rules.

A CBDC locking mechanism would allow users to earmark funds on the ledger via the API layer. The funds would be locked until a pre-defined condition has been met. These conditions might include:

- A set period of time has elapsed.
- A cryptographic secret is provided to the contract.
- A predetermined number of signatures needed to release the lock have been provided (ie multi-signature wallets).
- A trusted third party indicates that the agreed condition has taken place.

PIPs and ESIPs might facilitate and orchestrate the functionality, subject to end-user permission to instruct locks on the core ledger. PIPs and ESIPs would host contract logic on their own infrastructure, but would instruct the release of funds via API to the core ledger.[38] This may require such entities to integrate with other ledgers and databases to observe and retrieve data, similar to how an oracle functions within the crypto ecosystem.

If the set conditions are not met, all locks would have an expiry time where the funds are released back to the original owner to ensure no funds are locked indefinitely on the ledger.

Assuming that funds are locked until the pre-programmed conditions have been met, this approach might facilitate atomic settlement of PvP, DvP and smart contracts.[39]

There are various methods for enabling the locking process described, and the Bank does not have views on the overall desirability of a locking mechanism, nor any specific locking solution at this stage. Hash-time lock contracts have been popularised by cryptocurrencies in recent years, as have multi-signature transactions. Both of these mechanisms, alongside alternative and traditional approaches, could be considered as part of the design phase for a CBDC.

[38] This model is similar in principle to the proposed **Synchronisation** model for RTGS in the **Roadmap for RTGS beyond 2024**. By harmonising the regulatory and technical standards of these two models as far as possible, PIPs and ESIPs offering PvP or DvP may be able to act as Synchronisation Operators and vice versa.
[39] The Jasper-Ubin design paper explores this idea, we look to build on this concept through our own experimentation. **Jasper-Ubin Design Paper**.

Enabling programmability would raise a range of technology considerations which would need to be carefully evaluated.

Table H: Technology considerations related to programmability

Consideration	Description
Data usage and performance	Locking mechanisms require additional and more complex data to be stored and processed on the ledger. How does this impact performance?
Security	What are the security risks associated with locking mechanisms and how best can they be mitigated?
Standards	Which standards should be considered to ensure locking mechanisms are interoperable with services connecting to different ledgers?
Liability	Should a locking mechanism fail, or the function be disputed, what might a liability framework look like?
Benefit	The benefits of CBDC-based atomic swaps and smart contracts are conceptual at this stage. Are the benefits real and tangible?
Who can implement?	Should only permitted parties (PIPs, ESIPs) be able to implement CBDC smart contracts, PvP and DvP external services? If so, how would this be managed and regulated? What end-user consents would be required?

Next steps

Programmability and smart contract functionality could present significant benefits for users of CBDC and for innovation more broadly. As such, the Bank will undertake research and experimentation of such functionality in the design phase, including consideration of experiments and proofs of concept with private-sector firms and technologists.

4.8: Offline payments

Summary

- Offline payments, where transactions occur with both parties disconnected from the network, come with an increased risk of double spend.
- Double spend risk might be reduced by a combination of policy (eg limits for consecutive offline payments, local recording and online reconciliation of offline payments) and technology controls (secure hardware and potential cryptography mechanisms). These approaches require further analysis and experimentation to determine their viability and appropriateness.

Offline payments are transactions which occur when neither party has a network connection.

An offline payment is one that occurs while neither payer nor payee has access to the CBDC network, usually due to the lack of an internet connection.

A CBDC with offline payment functionality might provide additional resilience in the event of network disruption or outage of telephony services. The ability to make offline payments may also be beneficial in areas with low network connectivity, for some groups at risk of financial exclusion, or for certain payment use cases, such as transportation.

Trust in the CBDC system is key to its adoption, including the reliable verification of CBDC authenticity.

Verifiable authenticity controls for offline transactions are essential to reduce the risk of counterfeit CBDC, double spending and other forms of fraud. The authenticity of CBDC funds, including funds stored in offline wallets, might be validated using cryptographic primitives.

Double spending occurs where the same funds are spent more than once, and is particularly relevant in offline payments. As offline payments take place disconnected from the core ledger, it is more challenging to verify that funds have not already been spent at the point the payment is made.

It is yet to be determined whether the double spend risk could be completely eliminated for offline payments, but there are approaches which may reduce this risk.

There are several potential approaches to managing double spend risk, which might be used in combination. These include:

- **Risk prevention** (tamper-resistant hardware):
  Offline payments might be conducted on secure devices that reduce the likelihood of double spend. Existing card technology and most smartphones today are equipped

with secure hardware for the storage of private keys and sensitive data. Tamper-resistant hardware helps protect against private key compromise and double spend.

- **Risk minimisation** (offline limits):
  Offline limits might help to reduce the scale and impact of double spend. These limits, if implemented, might be based on the number of consecutive offline transactions, or they could be time or value based. Such limits would need to be considered in light of any liability framework for offline transactions. PIPs and ESIPs would likely have a role in the design of these limits, and be responsible for their implementation.
- **Risk detection** (transaction recording):
  Necessary payer and payee data could be recorded in offline transactions to support double spend detection and corrective actions. When a wallet involved in offline transactions reconnects to the core ledger, the transaction record stored locally could be reconciled, with any discrepancies highlighted for subsequent corrective action. Consistent with provisions to protect user privacy, any personal data gathered would be held by the PIP or ESIP, and subject to data protection requirements. No personal data would be held by the Bank.

> **Further analysis and experimentation is required to determine the most viable approaches.**

As offline payments cannot be recorded or reconciled against the core ledger at the point they take place, there could be different approaches to the recording of transactional data. Two possible approaches are:

- **Local transaction record:** Both devices participating in an offline transaction would keep a local record of the transaction. Where consecutive offline payments are made, a record of previous offline transactions could be passed along with each new offline transaction. This offline transaction record would then be recorded on the core ledger when any of the participating devices reconnects to the ledger.
- **No transaction record:** The details of offline transactions would not be recorded locally. Offline transactions would thus effectively be fully private. If double spending were to occur, there would be no way of knowing which device initiated it. This approach effectively enables anonymous payments, and is therefore unlikely to align with our approach to CBDC privacy.

Offline payments may introduce complexities that might impact the security and performance of a CBDC system.

Further work is needed to assess the technology and policy considerations involved in offline payments. In particular, the design and implementation of any limits on offline transactions needs careful consideration. These could introduce complexities in code and design that may increase the likelihood of software (and potentially hardware) vulnerabilities. Offline limits could also negatively impact the latency of offline transactions. This will need to be considered alongside any risk appetite for potential double spend events and consideration of a loss liability framework.

Next steps

The Bank will examine various approaches to managing double spend risk, spanning technology, operational, policy and legal implications.

The Bank will also analyse further the privacy implications and technology considerations around the local recording of offline transactions for reconciliation with the core ledger.

5: Next steps and discussion questions

The design of a UK CBDC poses a range of complex technology considerations and technical requirements. This paper sets out the Bank's emerging thinking and high-level approach to some of these considerations, informed by work in the research and exploration phase.

Our future work on CBDC, during the design phase, will focus on the technology considerations and associated trade-offs involved in CBDC design and their implications for our policy objectives as set out in the digital pound CP. This will include examining various approaches to meeting specific targets outlined in this paper, as well as assessing our technical requirements and determining the solutions that would best meet them. During the design phase, the Bank will develop a comprehensive conceptual architecture which can be used as a blueprint for building a UK CBDC, should we proceed to a build phase. The Bank will also conduct experimentation and proofs of concept, in collaboration with private sector innovators, to inform the development of the CBDC architecture and private sector's digital currency technology know-how.

Specific questions on some of these areas are listed below, and observations on other aspects are also welcome. We also encourage respondents to highlight, in their responses, any trade-offs or interdependencies between different aspects that may result from suggested solutions or approaches. We do not expect responses to address all questions. Details on **how to respond** can be found on page 7.

Technology design considerations

Based on the policy objectives outlined in the digital pound CP, the Bank assesses that privacy, security, resilience, performance, extensibility and energy usage are foundational technology considerations for CBDC (Section 3).

1. Do you agree that these six considerations are foundational technology considerations for CBDC? Are there additional or alternative technology considerations that the Bank should be focused on? (Section 3)
2. Which privacy-enhancing technologies, or other privacy mechanisms, might support the proposed policy objectives, and how might they be used? (Section 3.1)
3. Are the provisional requirements and metrics discussed in the paper, particularly for uptime, transaction throughput and transaction speed, realistic and appropriate? (Sections 3.3 and 3.4)

Illustrative conceptual model

The illustrative conceptual model features the core ledger, API layer, alias service and analytics as part of the Bank-managed infrastructure, while programmability and devices are featured as aspects of the CBDC ecosystem infrastructure. It also considers offline payments and interoperability with other forms of money (Section 4).

4. Are there other significant components or activities that the Bank should consider in designing a CBDC? (Section 4)
5. Are there alternative models that might better address the technology considerations and technical requirements outlined in this paper? (Section 4)
6. Other than those described in this paper, are there additional important factors to consider related to ledger design? (Section 4.1)
7. What are the most appropriate approaches or technologies for collecting and analysing aggregate transaction data? (Section 4.2)
8. Do you agree with the need for aliases (both well-known and disposable)? If so, should the alias service be hosted as part of the Bank-managed infrastructure, or should it be distributed across the CBDC ecosystem? (Section 4.3)
9. What features would a CBDC API require to enable innovative use cases? (Section 4.4)
10. Do you agree with the suggested list of devices for making payments with CBDC? (Section 4.5)
11. How viable is it to enable interoperability between CBDC and other forms of money using existing payments infrastructure? (Section 4.6)
12. Is programmability and smart contract functionality an important feature of a CBDC system? If so, what is the best approach to enabling such functionality? (Section 4.7)
13. How important is offline functionality in a CBDC system? What are the most effective ways to implement offline capability? (Section 4.8)

Public Sector Equality Duty

The Bank, in the exercise of its public functions, is subject to a statutory duty set out in the Equality Act 2010 (Equality Act) to 'have due regard' to equality considerations, comprising the need to: (a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act; (b) advance equality of opportunity between persons who share a relevant protected characteristic under the Equality Act and persons who do not share it; and (c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it (the Public Sector Equality Duty (PSED)). For the purposes of the design proposals for a digital pound, there are significant policy and technological decisions which would need to be taken to ensure fair and equitable access. As part of the policy development process, the Bank will undertake an Equality Impact Assessment in respect of the proposals, to ensure that appropriate consideration is given to matters set out in the PSED.

Privacy notice

By responding to this paper, you provide personal data to the Bank. This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform the Bank's work as a monetary authority, as a supervisor of financial services firms and as the central bank of the United Kingdom, both in the public interest and in the exercise of the Bank's official authority. The Bank may use your details to contact you to clarify any aspects of your response.

We will retain all responses for the period that is relevant to supporting ongoing financial services law and policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how we deal with your personal data, your rights or to get in touch please visit **Privacy and the Bank of England**.

Information provided in response to this paper, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000, or as otherwise required by law or in discharge of the Bank's functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank receives a request for disclosure of this information, we will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on the Bank.

Glossary

2PC – two-phase commit.

ABE – attribute-based encryption.

ACID – atomicity, consistency, isolation and durability.

AML – anti-money laundering.

API – application programming interface.

ATM – automated teller machine.

CBDC – central bank digital currency.

CDCVM – Consumer Device Customer Verification Method.

CP – Consultation Paper.

DDoS – distributed denial of service.

DLT – distributed ledger technology.

EMV – Europay, Mastercard and Visa.

ESIP – External Service Interface Provider.

EVM – Ethereum Virtual Machine.

FPS – Faster Payment System.

HM Government – His Majesty’s Government.

HM Treasury – His Majesty’s Treasury.

IoT – Internet of Things.

KYC – know your customer.

ML – machine learning.

P2B – person-to-business.

P2P – peer-to-peer.

PAN – primary account number.

PET – privacy-enhancing technology.

PIN – personal identification number.

PIP – Payment Interface Provider.

PIR – private information retrieval.

PoS – point of sale.

PSED – Public Sector Equality Duty.

RTGS – Real-Time Gross Settlement.

SCA – strong customer authentication.

SMPC – secure multi-party computation.

TWP – Technology Working Paper.

ZKP – zero knowledge proofs.

ZKRP – zero knowledge range proofs.