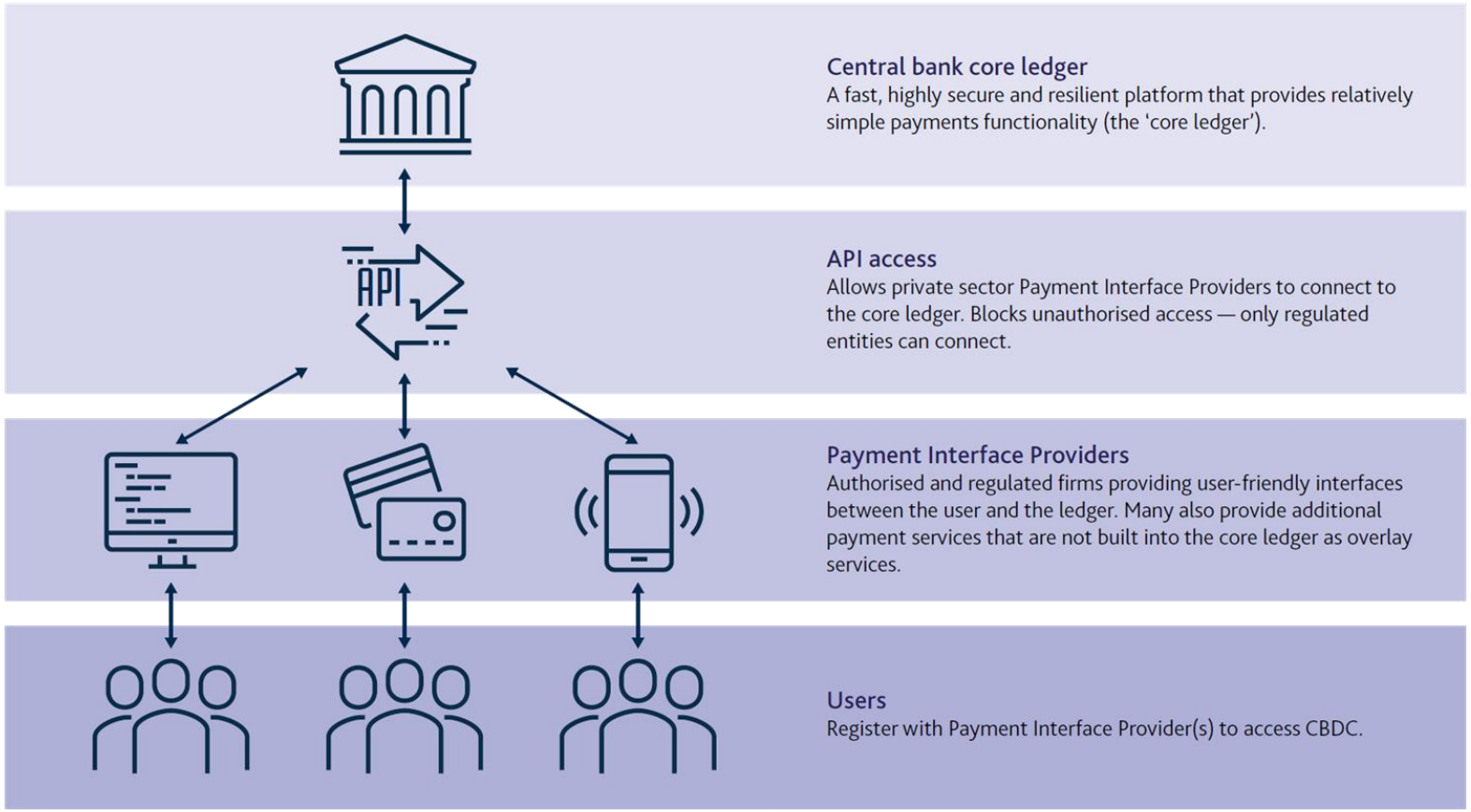
BANK OF ENGLAND

Item 2 - Models of CBDC Provision

CBDC Technology Forum
November Meeting

The platform model of CBDC



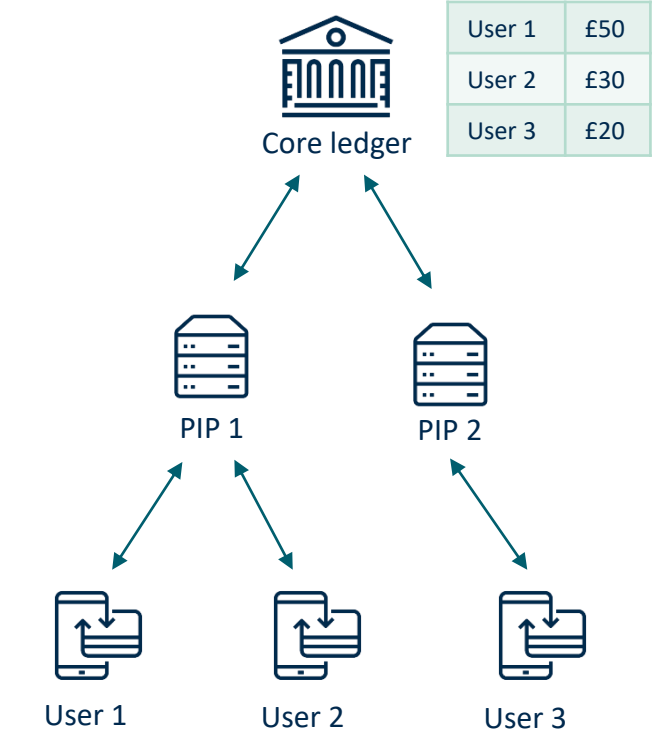
Central bank core ledger
A fast, highly secure and resilient platform that provides relatively simple payments functionality (the 'core ledger').

API access
Allows private sector Payment Interface Providers to connect to the core ledger. Blocks unauthorised access — only regulated entities can connect.

Payment Interface Providers
Authorised and regulated firms providing user-friendly interfaces between the user and the ledger. Many also provide additional payment services that are not built into the core ledger as overlay services.

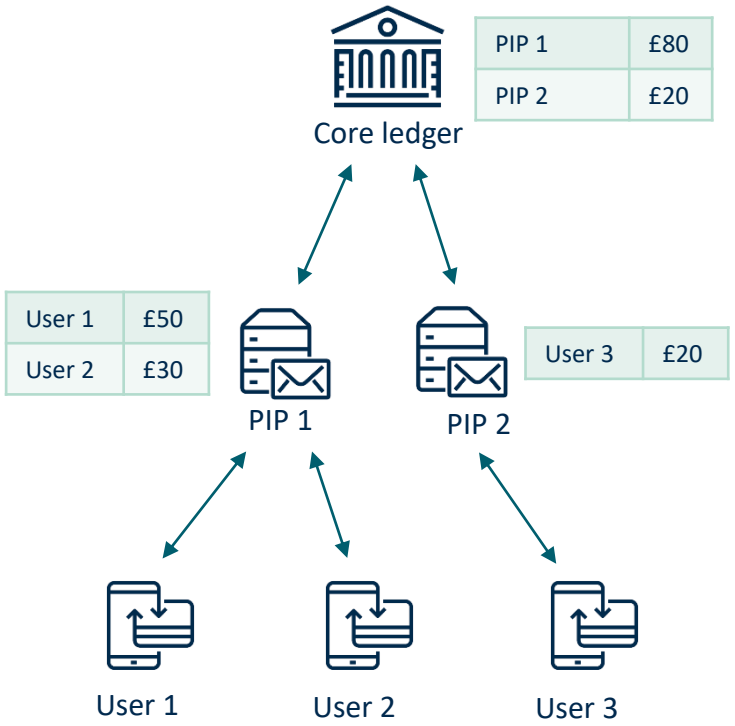
Users
Register with Payment Interface Provider(s) to access CBDC.

Platform Model

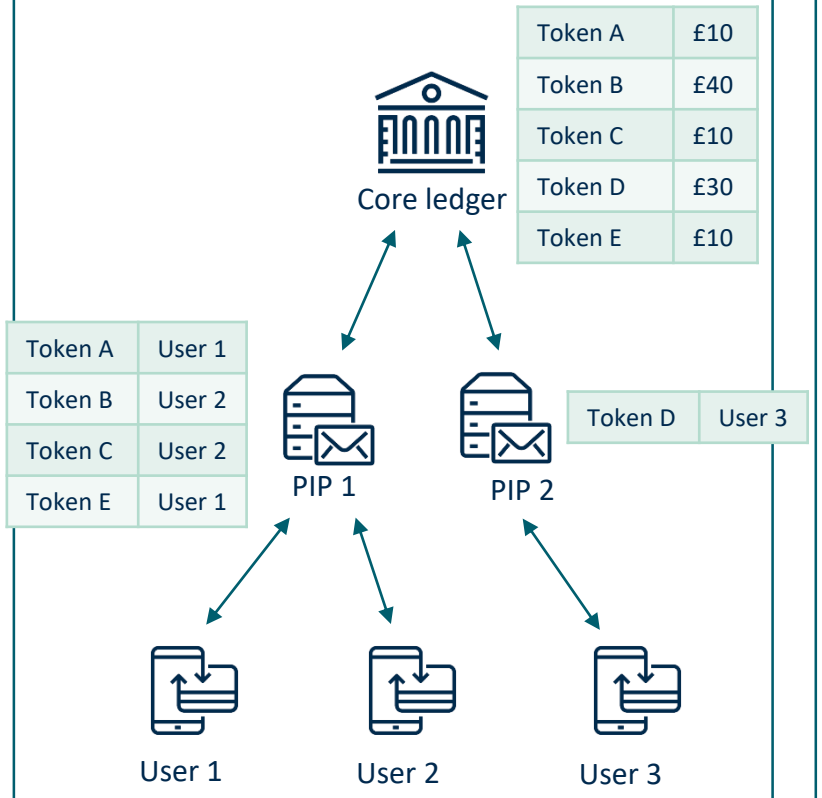


Further Models of CBDC Provision

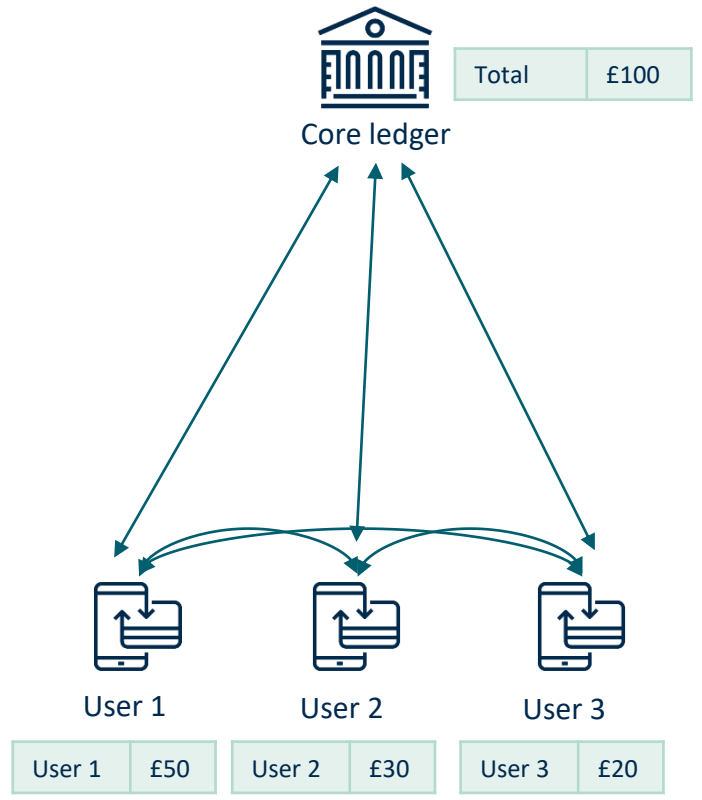
Pooled Account Model



Intermediated Token Model



Bearer Instrument Model



Responses to the Bank of England's March 2020 Discussion Paper

Principle 2: A competitive CBDC ecosystem with a diverse set of participants will support innovation and offer the best chance to deliver the benefits of CBDC

- The Bank should provide the minimum level of infrastructure for the system to be reliable, resilient, fast and efficient
- The private sector should take a leading role in responding to the needs of the end users, including competing to provide them with innovative 'overlay' services using the core CBDC infrastructure
- The Bank will continue to refine and develop the idea of a 'platform model' in its CBDC exploration

Member presentations

Questions for the Technology Forum

Q1: *Are all these models technologically feasible? Are they technologically distinct? Are there additional variations we should consider?*

Q2: *With what criteria should we evaluate these potential models of CBDC provision?*

Q3: *Which model attributes are critical in defining a given model, compared to those attributes which are non-specific to any given model?*

Q4: *Do any of these models have specific advantages over the others? For example: Performance advantages? Resilience advantages? Their openness to innovation and competition?*

Q5: *How do we resolve double spend risk within these models? Specifically, how do we solve double spend risk in bearer instrument models?*

BANK OF ENGLAND

Item 3 – Privacy in a CBDC system

CBDC Technology Forum – November Meeting

Privacy: Recap on responses to our Discussion Paper

Respondents offered a variety of different views:

Some respondents said their privacy and anonymity expectations were grounded in the example of cash, or taken from the principles and technologies underlying decentralised cryptocurrencies.

Other respondents recognised the challenges of balancing privacy and anonymity with the need to tackle financial crime and illicit finance behaviour.

Some feedback suggested the Bank should be guided by current and future regulations on data protection and Know Your Customer (KYC) in determining the appropriate level of privacy

Privacy: Recap on Bank's current position

- Privacy is of **critical importance**, but this is **not the same as anonymity**.
- The Bank will work closely with, and take its lead from, **HM Government** on issues of privacy.
- A CBDC would need to **comply with regulations** around anti-money laundering (AML), countering the financing of terrorism (CFT) and sanctions
- It is therefore likely that someone in the system would need **a way to identify users**. However, we may want the core ledger to record **pseudo-anonymous transaction data** only so that the central bank does not see sensitive data.

Member presentation

Questions for the Technology Forum

The Bank is not asking TF members for their views on the appropriate level of privacy in a CBDC system. Rather, we are interested in your insights around the data in a CBDC system and the possible architecture and technologies available to keep this data private.

Q1: *What are the main types of sensitive data generated/ required in a retail payments system such as a CBDC? Who would hold this data?*

Q2: *What are the biggest technical challenges in segregating and protecting this data, in order to ensure the privacy (not necessarily anonymity) of end-users?*

Q3: *Which are the most relevant privacy-enhancing technologies to consider?*

Q4: *Linking back to the earlier models discussion, which models of CBDC provision best support the use of privacy-enhancing technologies?*