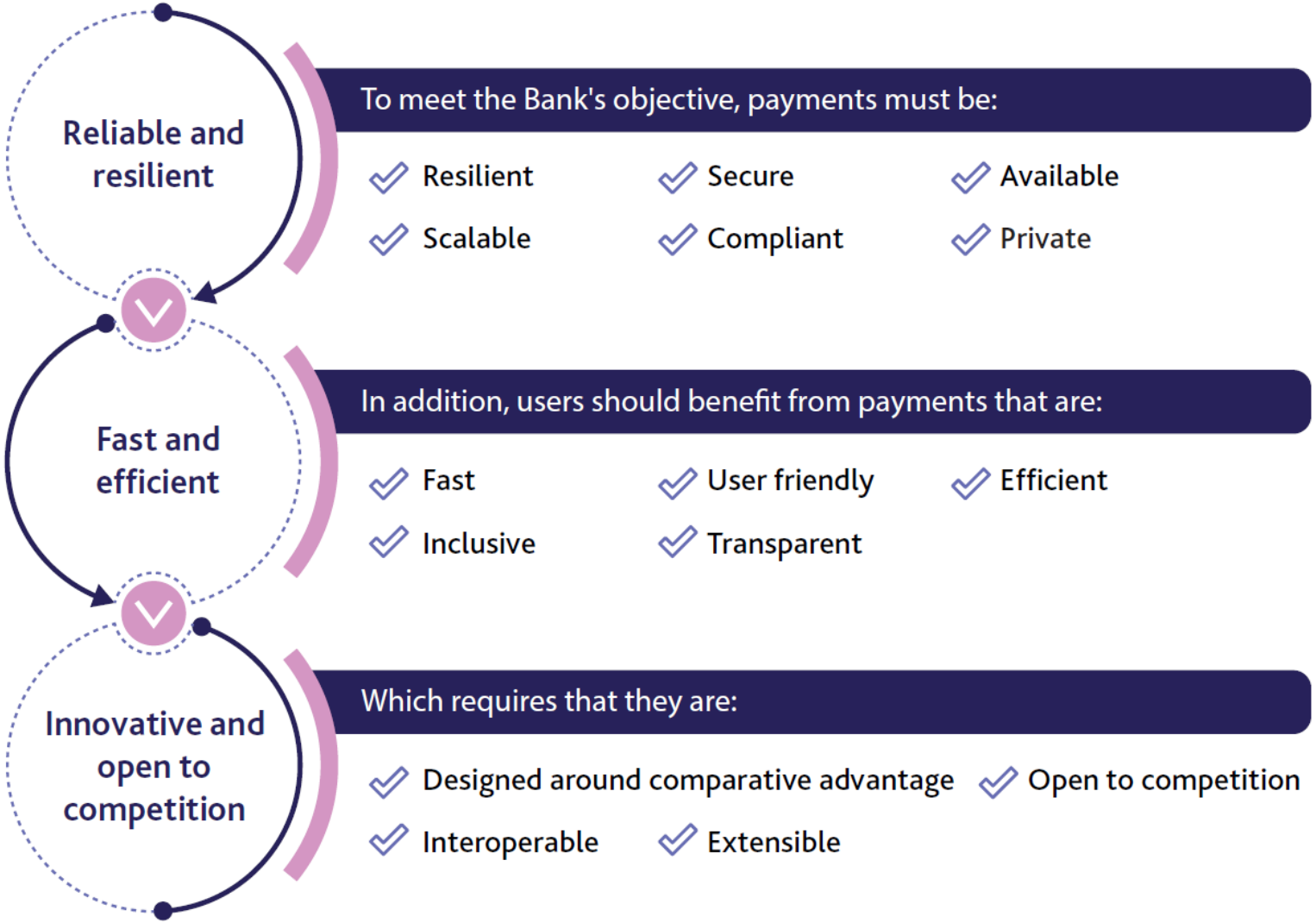
BANK OF ENGLAND

Item 2 - Recap of some assumptions around CBDC technology

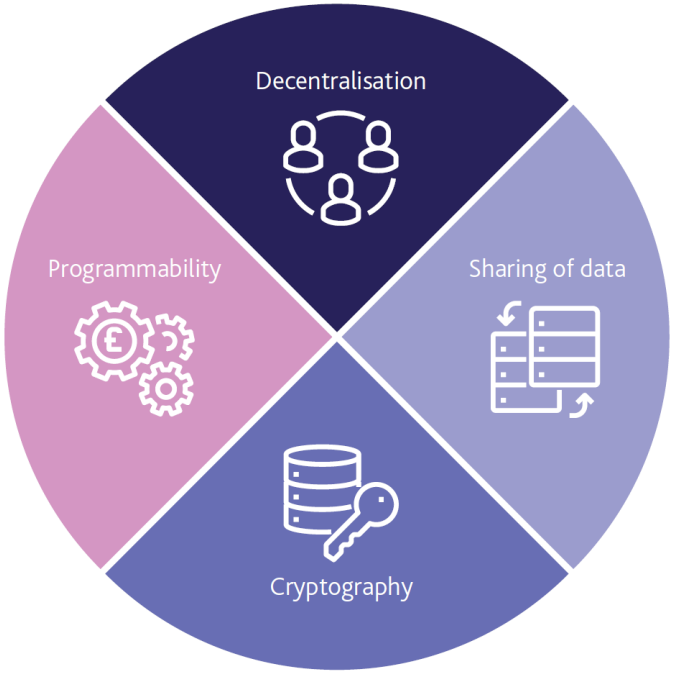
CBDC Technology Forum Meeting – September Meeting

Design characteristics of a CBDC system

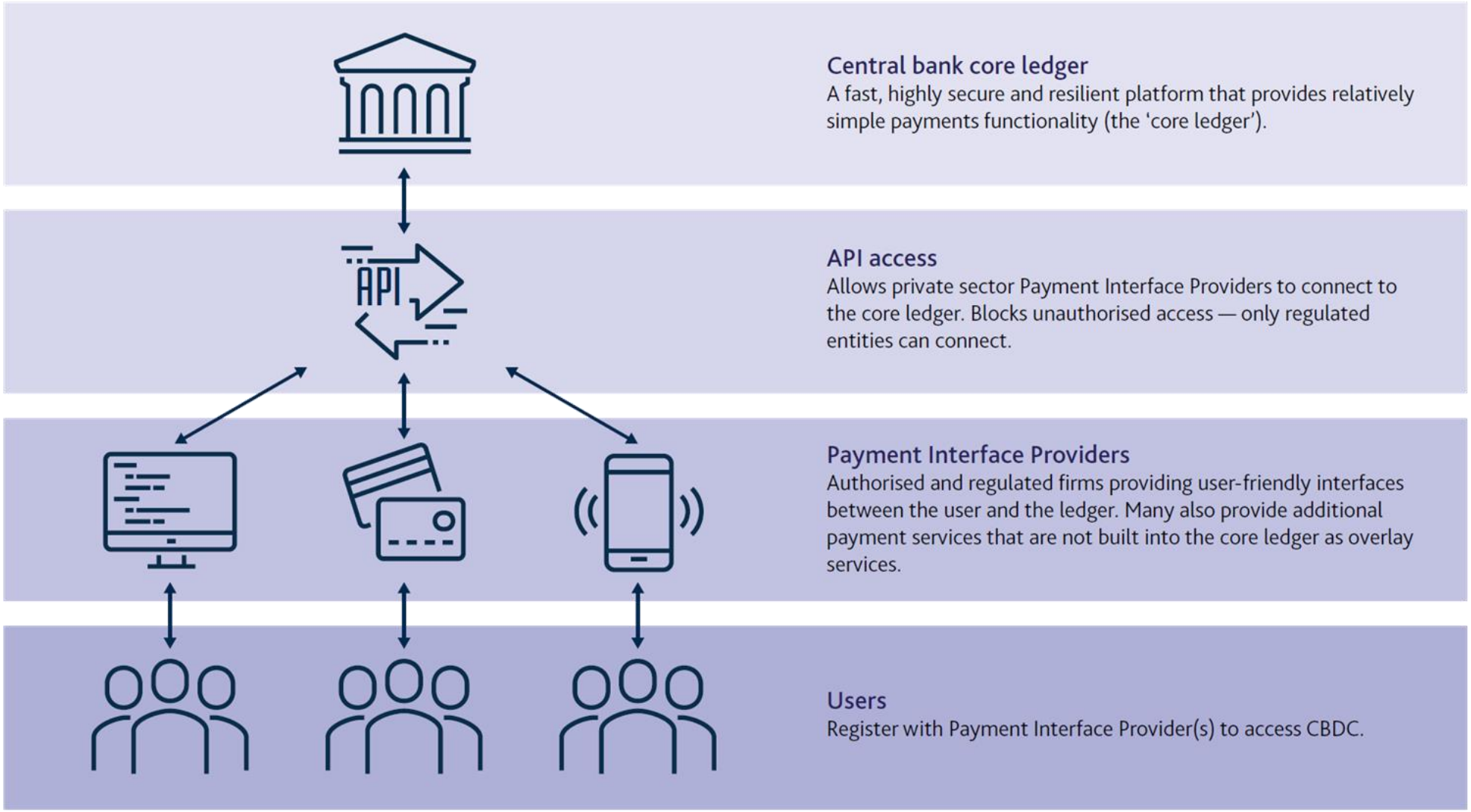


What technology might CBDC use?

- We remain technology agnostic in our design of a CBDC. In particular we do not presume a CBDC requires DLT
- We need to decide the required functionality before choosing a specific technology – *what* comes before *how*
- However, it is important to explore technology now, rather than waiting until we have finalised our *what*



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').

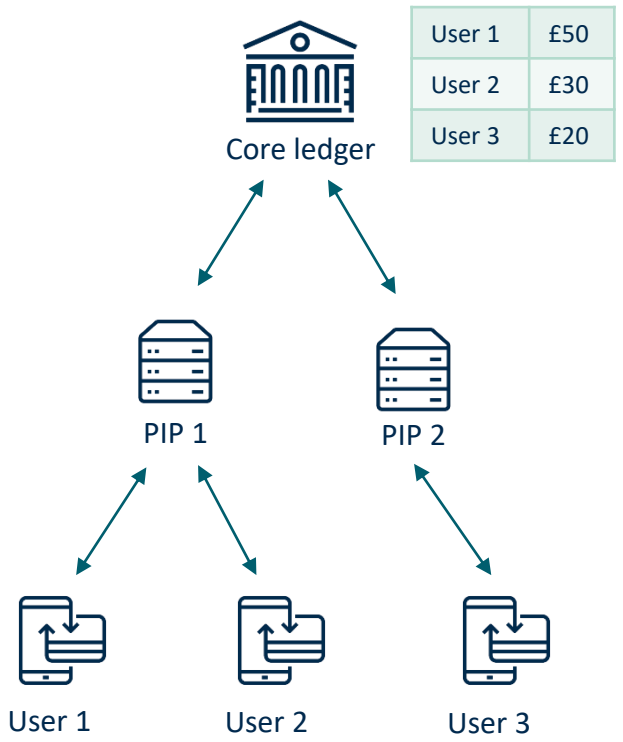
API access
Allows private sector Payment Interface Providers to connect to the core ledger. Blocks unauthorised access — only regulated entities can connect.

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.

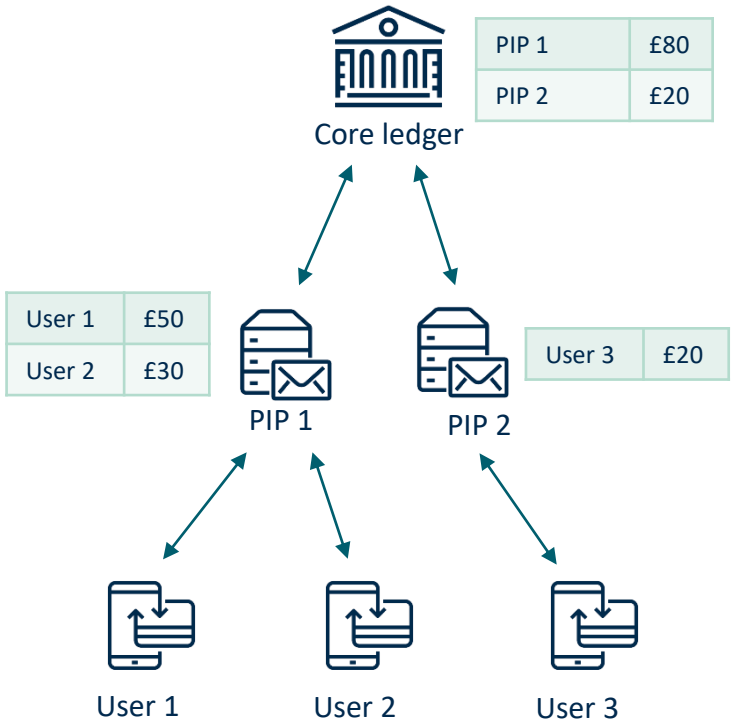
Users
Register with Payment Interface Provider(s) to access CBDC.

Models of CBDC Provision

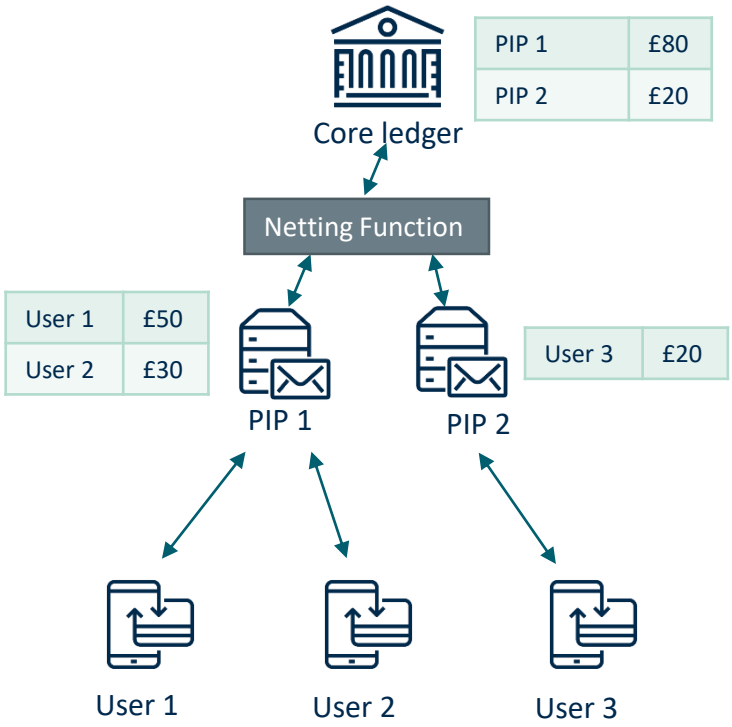
1 – Platform Model



2 –Pooled Model



3 – Pooled Model, Deferred Net Settlement



Ledger design – (de)centralisation

- All ledger structures remain on the table – we have no assumption of DLT (nor any other tech)
- Any solution will need to meet a range of necessary requirements – in particular around resilience, availability, security, speed, throughput and scalability
- The ledger will be recording liabilities of the Bank, so the Bank would need a degree of control or oversight. But a ledger design could include elements of distributed approaches

Ledger design – accounts & tokens

- “Token” versus “account” is not a debate to have in isolation – this choice will emerge from requirements
- Our interpretation of the key distinction relates to the data structure – i.e. whether units of value are moved between different owners (“token”), or whether account balances are increased or decreased (“account”) – but there are other interpretations
- We are yet to identify specific functionality that is unique to either approach. Instead of focusing on the labels, we should look at the approach(es) which best deliver the necessary functionality

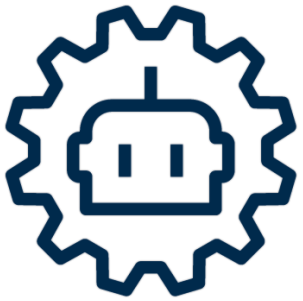
Privacy

- Privacy is of critical importance, but this is not the same as anonymity
- 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, where possible, we may want to record pseudo-anonymous transaction data only

Online vs offline payments

- Our assumption is that the primary “mode” for a CBDC would involve an active network connection, with users and intermediaries communicating with the CBDC network (i.e. *online*)
- However, there may need to be some ability for *offline* transactions (i.e. where neither party is connected to the network) in certain circumstances – but this may not be core, or “day 1” functionality
- There appear to be potential technology solutions here, but none of which avoid the introduction of some amount of risk, requiring mitigation in the form of limits and clear delegation of liability

Programmability



- There are different degrees of “programmability” a CBDC system could enable.
- This functionality might therefore be deployed in different parts of a CBDC ecosystem (e.g. in the core ledger vs external applications)
- It may be preferable for this functionality to sit outside the core architecture, to minimise security risks and complexity of the ledger
- Programmability may not be a “day 1” requirement, but at a minimum we will need to design CBDC with future flexibility and extensibility in mind

Simplicity

- As a general principle, the core ledger infrastructure should be kept as simple as possible, with more complex functions provided as overlay services
- This simplicity may help enable higher performance, greater security, and greater extensibility
- We also recognise that the adoption of standardised protocols and messaging standards will be key to enabling interoperability, promoting financial inclusion and market competition, as well as to better manage security and regulatory risks