**Week 10 Seminar Solutions**

1. What is ‘Synthetic CBDC’? Is it a CBDC?

‘Synthetic CBDC’ is not a CBDC

A potential alternative framework under which central banks could engage with the rise of digital currencies would be for private sector payment service providers to issue liabilities matched by funds held at the central bank. Such an approach has been suggested by some stablecoin proposals and described in some papers as ‘synthetic CBDC’.

These payment service providers would act as intermediaries between the central bank and the end users. If the regulatory framework can guarantee that these providers’ liabilities will always be fully matched by funds at the central bank, these liabilities could share some of the characteristics of a CBDC issued by the central bank. Yet these liabilities would not be a CBDC, as the end user would not hold a claim on the central bank. They are, essentially, a form of “narrow-bank” money.

In addition to not being a CBDC by definition, these liabilities would also lack some key features of central bank money. Commercial payment service providers benefit from strong network effects, potentially leading to concentration and monopolies or fragmentation. Central banks have public policy, rather than profit objectives. This enables neutrality in providing services to users, allowing for an open and inclusive system.

Another difference between CBDC and narrow-bank money is liquidity. Central banks can expand their balance sheets and create additional liabilities, at short notice, in response to underlying demand. By design, a payment service provider as described above cannot do this – every liability must be matched by funds held at the central bank. This makes a CBDC more liquid than a matched claim on a private provider. For narrow-bank money, concerns about the existence of the underlying matched funds could cause doubts on the value of the liabilities and result in users selling them at a discount to the par value of the currency. This cannot occur with a CBDC.

There might be a useful role for privately issued liabilities matched with central bank money in a jurisdiction’s payment system. However, the necessary information and decision-making process for a central bank to enable such an arrangement is very different from a consideration of issuing CBDC.

Explain the following CBDC technology considerations.

2. Convenient

Achieving tap-to-pay for users with relatively modern smartphones, stored value cards and custom devices fitted with near field communications (NFC) is straightforward and well understood. However, depending on the jurisdiction, the availability of NFC or fitted cameras on smartphones to read QR codes could be used. A variety of user-friendly payment options may be needed to support differing use cases (eg e-commerce or person-to-person payments).

For users without smartphones, central banks (or customer-facing termediaries)

could offer devices (eg stored value cards or more interactive devices with displays) designed for point of sale terminals, online and device-to-device transactions. Dedicated devices could also support offline transactions. To support users with cognitive, motor or sensory impairments, engagement with representative user groups and design experts should guide development.

3. Secure and Resilient

To protect user data, there are a variety of mature cryptographic techniques flexible enough to be used across centralised or distributed ledgers. Typically, in a centralised platform, it is the system administrator who enforces privacy policy, while distributed or device-based environments with less straightforward governance arrangements can face complications from software-based privacy enforcement. For local store of value style systems, technologies such as

tamper-resistant hardware found in credit cards and smartphones today do store other forms of sensitive data and may be a suitable basis on which to provide local CBDC security.

As critical infrastructure, the resilience of CBDC will likely need to be similar to current payment systems and operate a 24/7/365 service. While in principle distributed ledger technology (DLT)-based systems may offer resilience benefits, by replicating data over many more computers, so could a centralised ledger with a small number of data centres.

4. Fast and Scalable

The CBDC system will need to be able to meet the volume and throughput (transactions per second) requirements at a justifiable cost. Ideally, volumes can drive marginal costs to extremely low levels. Existing large centralised systems (eg card networks) demonstrate that very high transaction capacity for large populations is possible with conventional technologies.

Research on scalability has shown that performance problems associated with public DLT networks (that require mining or other consensus protocols) can be overcome with permissioned DLT networks. Nonetheless, estimating current and future volumes and throughput requirements for a CBDC is complicated and exacerbated by other industry developments (eg payment requests generated by smart devices and the potential for high volume micro transactions).

5. Interoperable

Technologies to support platform business models, allowing third parties to build services on top of a CBDC system, are well established (eg use of application programming interfaces (APIs)). The challenge in interoperating with existing payment arrangements will depend on their designs but most have standardised mechanisms to make inter-account transactions.

Common data standards, most notably ISO 20022, will likely play a part in enabling interoperability with other payment systems. In a CBDC system with intermediaries, its design will need to support payments (be it online or offline) between customers of one intermediary and those of another and support portability, to avoid users being locked in to a single intermediary.

6. Flexible and Adaptable

Several factors determine how adaptable a CBDC system is: how accurately the fundamental concepts of money and payments are enacted; a careful, layered design with a clear separation of concerns; designing with foresight into how the environment may evolve (eg micro transactions, changes in cryptography) and so on.