



PART 3

Read the text below and answer questions 27–40.

CENTRAL BANK DIGITAL CURRENCIES: A MONETARY REVOLUTION?

A central bank digital currency (CBDC) is often described as “digital cash”, but the label can obscure what matters most. The defining feature is not whether the system uses a blockchain, a database, or some hybrid architecture; it is the issuer and the legal claim. A CBDC is a digital form of money that is a direct liability of the central bank. That status distinguishes it from commercial bank deposits, which are claims on private intermediaries, and from private crypto-assets or stablecoins, which depend on issuer reserves or algorithmic mechanisms rather than state-backed fiduciary authority. Interest in CBDCs has risen as payment activity shifts toward a small number of private networks, raising concerns about monetary sovereignty, market concentration, and the resilience of national payment rails if a dominant platform fails.

Design debates quickly move from definition to architecture. A common distinction is between wholesale CBDCs and retail CBDCs. Wholesale versions target banks and other financial institutions, with the aim of improving settlement for large-value transfers, reducing counterparty risk, and potentially increasing efficiency in securities or interbank markets. Retail versions are intended for households and firms, and therefore involve consumer onboarding, dispute resolution, accessibility, and day-to-day usability. Because most central banks are not designed to operate as customer-facing service providers, many proposals adopt a two-tier model in which the central bank issues the instrument, but private intermediaries deliver wallets, identity checks, and customer support. The objective is to preserve the advantages of a public liability while relying on existing distribution channels, and to reduce the risk of disintermediation in which deposits migrate suddenly from banks to the central bank.

Privacy is often presented as the most politically sensitive design choice, because it sits at the intersection of civil liberties and financial integrity. Physical cash can be used with a high degree of anonymity, but replicating that feature in digital form at scale is difficult without creating channels for illicit finance. As a result, many designs explore “privacy by design” approaches combined with legal safeguards, tiered identity requirements, or limited-value anonymous functionality. The practical outcome depends not only on cryptographic techniques but also on governance: what data is collected, who can access it, how long it is stored, and under what legal thresholds it can be disclosed. A technically elegant system can still be experienced as intrusive if oversight is weak or if access rules are opaque.



Programmability adds a second layer of controversy, partly because the term is used in different ways. Some advocates use it to describe smart features at the payment layer: automatic tax withholding, conditional transfers for targeted subsidies, or machine-to-machine payments in logistics and energy systems. Critics worry that “smart money” could become money that is controllable in socially coercive ways, such as restricting what can be purchased or imposing expiry dates. Many central banks respond by drawing a boundary between the currency and the surrounding applications. They argue that broad spending rules should be applied at the wallet or account level, through regulated intermediaries and due process, rather than being embedded as restrictions in the base unit of money itself. In this framing, CBDCs can support innovation in payment services without turning the currency into a tool for general behavioural enforcement.

Financial stability is another recurring concern, especially in systems where retail CBDCs would be widely accessible. If households can hold central bank money directly in digital form, they may shift funds away from commercial banks, particularly during periods of stress when safety is valued over return. That could shrink bank funding, raise the cost of credit, and accelerate the dynamics of a bank run, because conversion from deposits to central bank money could occur at high speed. To manage this risk, proposals often include design tools such as holding limits, tiered remuneration, or conversion frictions for large movements. For example, balances above a threshold might earn a low or zero return, discouraging large-scale parking of funds while keeping the CBDC usable for everyday payments. Such mechanisms reflect a balancing act between convenience and systemic liquidity risk.

Cross-border payments are frequently cited as a motivation for CBDC development, particularly because existing international transfers remain slow and costly. Correspondent banking chains involve multiple intermediaries, repeated compliance checks, time-zone frictions, and settlement delays. In theory, interoperable CBDCs could shorten settlement paths by reducing the number of hops between payer and recipient, improving transparency and potentially lowering fees. Yet the obstacles are institutional rather than purely technical. Interoperability requires agreement on standards, identity frameworks, legal recognition, exchange mechanisms, and oversight responsibilities. National interests often diverge on these issues, especially where capital controls, data rules, or sanctions regimes are involved. As a result, cross-border gains are plausible but contingent on coordination that may be politically difficult.

Operational risk may be the most underestimated challenge, because a widely used CBDC would become critical national infrastructure. That status increases the consequences of outages and makes the system a high-value target for cyberattacks. Resilience planning



therefore extends beyond cryptography to include redundancy, stress testing, incident response capacity, and clear governance for emergency decisions. Some designs propose offline functionality so that limited payments can occur when connectivity fails, for example during network outages or natural disasters. However, enabling offline use can introduce new fraud risks and may require secure hardware, raising cost and implementation complexity. These trade-offs help explain why many central banks treat CBDCs as long-term projects, relying on pilots and staged rollouts rather than promising rapid transformation.

Questions 27–31

Select the correct answer.

27 What is the defining feature of a CBDC, according to the passage?

- A** It uses blockchain technology.
- B** It is a liability of the central bank.
- C** It is issued by commercial banks.
- D** It is backed by private reserves.

28 Why do many proposals prefer a “two-tier model”?

- A** To replace intermediaries completely.
- B** To make the central bank responsible for customer service.
- C** To keep intermediaries customer-facing while the state issues the money.
- D** To avoid any form of identity checking.

29 What does the passage emphasise about privacy in a CBDC?

- A** It depends on governance as well as technical design.
- B** It can match the anonymity of cash without enabling illicit finance.
- C** It is determined mainly by how quickly payments are settled.
- D** It requires central banks to store all user data indefinitely.

30 Which measure is described as a way to reduce financial stability risks?

- A** Removing all limits on holdings.
- B** Making the CBDC fully anonymous at any value.
- C** Requiring all deposits to be converted into CBDC.
- D** Setting holding limits or tiered remuneration.

31 What potential benefit of interoperable CBDCs is mentioned for international transfers?



- A** Ending the need for compliance checks.
- B** Shortening settlement paths in cross-border payments.
- C** Eliminating exchange-rate movements.
- D** Guaranteeing identical national standards.

Questions 32–36

Choose **TRUE** if the statement agrees with the information given in the text, choose **FALSE** if the statement contradicts the information, or choose **NOT GIVEN** if there is no information on this.

- 32** The passage states that CBDCs will replace cash in most countries within ten years.
- 33** The passage suggests that privacy outcomes depend on governance as well as technology.
- 34** The passage states that programmability has only one accepted meaning.
- 35** The passage suggests that central banks generally support embedding broad spending restrictions directly into the CBDC itself.
- 36** The passage indicates that interest-like design tools can be used to manage large CBDC holdings.

Questions 37–40

Complete the notes below. Choose **NO MORE THAN TWO WORDS** from the text for each answer.

CBDCs: key ideas

- A CBDC is defined as a digital form of money that is a direct **37** of the central bank.
- Many systems adopt a **38** so intermediaries can provide wallets and customer services.
- To cap the amount of CBDC a user can retain, proposals may impose **39**
- Supporting offline payments securely may require **40**

Answer Key

27. B

28. C



29. A

30. D

31. B

32. NOT GIVEN

33. TRUE

34. FALSE

35. FALSE

36. TRUE

37. liability

38. two-tier model

39. holding limits

40. secure hardware