Tokenizing central bank money on public blockchains[1]

U. Bindseil, B. Duve

23. August 2026

Abstract

We revisit issuing tokenized central bank money on public blockchains. Although central banks have debated CBDCs ("central bank digital currencies") for over a decade, policy efforts have mainly converged on centrally managed, ledger-based payment instruments, often constrained by concerns regarding privacy, financial stability, operational resilience, and the role of private payment providers. Meanwhile, private stablecoins on public blockchains have expanded rapidly, benefiting from global 24/7 infrastructure, composability, and smart-contract functionality, and many expect this trend to continue. Central banks have expressed concerns that stablecoins may threaten financial stability, foster illicit payments and dollarization, and weaken monetary sovereignty. Yet little attention has been given to placing sovereign money directly on public blockchains. Such an architecture is likely less costly to build and operate than a proprietary system, because it reuses existing open infrastructure and a widely available technology ecosystem, while supporting provider substitutability and reducing vendor lock-in, although issuer-specific control costs remain. The paper reviews the main challenges this model faces, assesses how modern blockchain features may mitigate risks, and evaluates the public policy objectives such issuance could advance.

Keywords: central bank money, tokenization, public blockchains, stablecoins

JEL-Codes: E50, E58, F30, F41

[1] We would like to thank for helpful comments Omid Malekan, Fabrice Rajaofera, Nacho Terol and Erwin Voloder. Views expressed are our own ones, not the ones of our present or past employers. All remaining errors are ours.

1. Introduction

The idea of tokenizing central bank money for distribution on public blockchains has found relatively limited attention over the last years. Instead, two other topics dominated public debate on the future of money:

(I) Central banks have extensively discussed the idea of issuing CBDC ("central bank digital currencies") for more than 10 years, but this mostly led to the conclusion to issue central ledger based, POI and P2P payment instruments. CBDC projects have had to balance public-policy objectives with concerns regarding privacy, financial stability, operational resilience, and the role of private payment providers. As a result, many designs are deliberately constrained, and deployment for POI and P2P payments has not been a large-scale success so far. This paper does not argue against these efforts but asks whether they should be complemented by central bank money issued on public blockchain rails.

(II) Stablecoins, i.e. private money on blockchain, has gained ever growing prominence in recent years, and it is generally believed that they will play a prominent role in the future as money: not only as global means of payment and store of value, but potentially also as retail payment instrument. Public blockchains with their omni-asset capability, 24/7 global availability and smart contract functionality can provide a low marginal cost opportunity to achieve universal access to tokenized assets, including tokenized money, and various use cases. Central banks have expressed some worries about stablecoins: that they could cause financial instability (for example when a run on them forces them into large scale asset liquidation), and that they could undermine monetary sovereignty by promoting dollarization and contribute to the crowding out of public money.

Central banks should not give up issuing banknotes, nor pursuing CBDCs for POI and P2P purposes using conventional technology. Central banks should however also consider issuing central bank money on public blockchains, i.e. combining the strength of central bank money (e.g. in terms of financial stability, generation of seigniorage income, allowing design decisions that directly follow public policy objectives, including preventing the use for illicit payments, strengthening monetary sovereignty, etc.) with the advantages of public blockchains that are considered to allow for the various use cases for stablecoins. Issuing CBDC on public blockchains ensures to not miss out on the promises of this new technology. The point is not to exclude regulated private or foreign providers of on-chain money, but to ensure that domestic public money can also operate on the same digital infrastructure. Benefiting from this new technology ensures to also preserve the benefits of central bank money for society under the scenario of an ever-increasing adoption of blockchain technology for payments. It can of course not address the problems of a fundamentally unstable currency: if inflation rates in a currency are very high because of a failed monetary policy, then residents will still seek dollarization and prefer holding e.g. USD stablecoins to domestic central bank money tokens.

This question is particularly relevant for countries already exposed to currency-substitution pressures. Foreign-denominated stablecoins may become attractive not only because users seek exposure to a foreign unit of account, but also because these instruments are increasingly easy to hold, transfer, and integrate into digital commerce and everyday payments. We do not argue that tokenizing domestic central bank money would displace demand for foreign unit-of-account exposure where that demand is driven by

domestic monetary instability. But it can make efficient use of the payment and settlement layer, namely the wallets, rails, and merchant integration, currently developed for foreign private stablecoins. Even where users retain foreign-currency exposure, there is no reason for the domestic payment and settlement layer to be conceded by default to foreign-denominated stablecoins or closed private payment schemes. Convenience and providing alternatives to foreign currency payment solutions are sufficient justifications for central banks to explore the discussed alternative. This is particularly true for central banks with limited budgets for payment infrastructure: public blockchains provide settlement rails whose development, operation, and global reach are financed by the network rather than by the issuer. The relevant question is whether central bank money can make use of the same type of cost-efficient and easy to deploy infrastructure that has enabled stablecoins to scale, while preserving central bank control over issuance, redemption, compliance, and final settlement. Issuer-specific control costs would remain, including governance, key management, compliance analytics, accounting integration and reconciliation, cybersecurity, legal processes, incident response and specialist operational capacity. These functions can, however, build on standardized protocols, open-source components, widely available tools and a competitive provider ecosystem rather than a proprietary technology stack developed and maintained primarily for the issuer. The central bank would also avoid funding the underlying network infrastructure itself. At the system level, reusable wallet infrastructure and software-based merchant acceptance on existing devices could further reduce deployment and operating costs. Taken together, these factors make materially lower issuer and system costs likely relative to a bespoke proprietary architecture, although the ultimate advantage depends on design requirements, network conditions and the extent to which control, resilience, offline and user-support functions must be recreated.

By “public blockchain rails”, this paper refers to public blockchain infrastructure (including selected Layer-1 networks, Layer-2 networks, and stablecoin-oriented payment chains) that allows tokenized money to circulate through open wallet, merchant, developer, custody, compliance, and settlement infrastructure. The term refers to the infrastructure layer only; it does not imply permissionless issuance: the central bank retains exclusive control over minting, redemption, canonical supply, and compliance. The proposal is thus to build public rails while retaining issuer control, the same combination that has allowed regulated stablecoins to operate at scale on these networks.

Previous discussions specifically of CBDC on public blockchain are relatively rare and include ConsenSys (2020) and Zhang and Huang (2022). We provide an updated and more comprehensive review of the topic. Section 2 reviews the concerns that central banks have expressed regarding central bank money on public blockchain. Section 3 argues that these concerns may be mitigated through various technical features that modern blockchains can offer, and that have been applied already for stablecoins. Section 4 concludes. Annex 1 discusses the central bank balance sheet and monetary income implications of new forms of money, including CBDC, and explains the income generation through CBDC.

2. Central banks' concerns on issuing central bank money into public blockchains

2.1 Technical limitations and fragmentation of public blockchains

Buterin (2015), (2017), (2021) identifies a "blockchain trilemma", an inevitable trade-off between decentralization, security, and scalability, as a central technical constraint when contemplating the issuance of central bank electronic money tokens (CEBMTs) on public blockchains. The trilemma suggests that no public blockchain can simultaneously maximize all three dimensions, implying unavoidable compromises in throughput, settlement assurance, or governance resilience. For a central bank, this raises the question on which chain should sovereign tokens circulate, and according to which performance and risk criteria? The dilemma is compounded by the fragmented nature of the public blockchain ecosystem. As the Bank for International Settlements (BIS 2023) notes, distributed ledger environments are characterized by interoperability frictions and limited native cross-chain composability, which may necessitate bridge mechanisms or parallel issuance across multiple chains. While a multi-chain strategy would mitigate vendor lock-in and enhance functional reach across heterogeneous use cases (retail payments, DeFi settlement, tokenized asset markets), it would also expand operational complexity, increase monitoring burdens, and multiply cybersecurity exposure, particularly where third-party bridge protocols are involved, which have historically proven vulnerable to exploits (BIS 2023; Federal Reserve Board 2022).

A seemingly straightforward solution, deploying a token via an ERC-20 smart contract on the Ethereum blockchain, has likewise been scrutinized. As Nyffenegger (2024, 544) observes, such an approach would subject the central bank to externally determined protocol rules and governance updates, potentially constraining monetary sovereignty at the infrastructure layer. Moreover, transaction fees, latency in finality, and the public transparency of ledger data may conflict with retail payment efficiency and privacy expectations. The BIS (2022) similarly cautions that public blockchains may struggle to meet the performance, scalability, and compliance requirements expected of sovereign monetary infrastructure. Proposed technical mitigations include Layer-2 "roll-up" architectures to enhance throughput while anchoring security in the base layer; yet these solutions introduce additional dependency layers and governance considerations. Although these limitations are not unique to central bank tokens, since private stablecoins operate under comparable infrastructural constraints and are projected to expand significantly (Citi 2025), the sovereign nature of CBDC heightens sensitivity to fragmentation, governance risk, and infrastructural dependence.

2.2 Safety and operational risks associated with public blockchain

Concerns relating to information technology security and operational resilience have figured prominently in central bank assessments of public blockchain-based CBDC architectures. As Khan and Malaika (2021) emphasize, distributed ledger systems are not inherently secure: applications deployed on public blockchain infrastructures remain susceptible to conventional software vulnerabilities and architectural flaws, while permissionless designs introduce additional attack vectors, including majority-consensus (so-called "51 percent") attacks. They caution that DLT systems are not "secure by default" and therefore

require rigorous risk management, particularly with respect to cryptographic key management, which constitutes the core authentication and authorization mechanism in token-based systems. For central banks, IT security risks could entail amplified systemic and reputational consequences, given the sovereign status of the issuer. Moreover, the so-called immutability of public blockchains creates legal and governance tensions where transactions are subsequently deemed unlawful or subject to reversal.

Complementing this analysis, the Federal Reserve Board (2022) observes that many advantages of permissionless architectures coexist with demonstrated security incidents, underscoring persistent vulnerabilities. It further notes that risk identification in DLT-based CBDC systems is complicated by the evolving nature of the technology and the limited empirical incident data available, thereby impeding robust comparative risk assessment across centralized, federated, and decentralized models. An important design question is the allocation of responsibility for cybersecurity controls in distributed environments, since effective protection presupposes clarity regarding ownership of risks and assets to be secured. The Federal Reserve also highlights the need to assess platform-specific cryptographic protocols against standardized and future-proofed alternatives, including potential quantum-resistant schemes. Finally, the distributed governance structure of public blockchains implies that security assurance cannot rely solely on a single operator but requires coordinated standards, supervisory oversight, and incident information-sharing mechanisms.

2.3 Financial-stability concerns and industry push-back

In the context of retail CBDC, the risks of disintermediating banks have been discussed extensively, with the banking industry arguing that CBDC could endanger banks' stability and their ability to provide credit. Surprisingly, such risks were never deemed relevant in the context of banknotes, although banknotes have the same effects on bank deposits as CBDC would have, and banknotes for example significantly increased for years at a pace above nominal GDP in the context of low interest rates (2008-2021). Bank disintermediation is nevertheless a concern that central banks have acknowledged. Holding limits, non-remuneration, and other constraints have been considered by many central banks; such features may be justified in some contexts, but they should not be treated as universal design principles before meaningful demand exists. On remuneration, two distinct perspectives have been advanced: (I) Some monetary macroeconomists (Barrdear and Kumhof, 2021) argue that remuneration could strengthen the transmission of monetary policy by using the interest rate on CBDC as an additional, non-redundant instrument. (II) Others, like Bindseil and Senner (2023), argue that remuneration would align the yield on central bank money with the interest rate cycle, as is the case for all other nominally defined financial assets, and propose a two-tier remuneration of CBDC to control against the risks of CBDC as a possibly disproportional store of value.

So far, CBDC deployment by central banks has not been a large-scale success. Industry stakeholders, who partially appear to have vested interests against CBDC, have raised broader concerns about CBDC, including privacy, financial stability, implementation costs, and the possible duplication of existing private payment services. These concerns can be and have been considered in design choices. At the same time, the rapid development of private digital payments and stablecoins suggests that central bank money

should not be excluded from technological modernization and in the past, central bank money remained unlimited as well, as do other forms of money.

2.4 Concerns that illicit use of stablecoin creates reputation risks for central banks

The evidence on the illicit use of stablecoins allows us to assess the potential reputational risks of issuing CBDC on a public blockchain. Recent empirical analysis by blockchain forensics firms indicates that stablecoins now account for a substantial share of illicit on-chain activity, including sanctions evasion, ransomware payments, fraud, and organized crime-related transfers (Chainalysis 2026; TRM Labs 2026). The Financial Action Task Force (FATF) has likewise observed that stablecoins are increasingly present in illicit transaction flows, warning that rapid adoption without consistent supervisory frameworks may amplify money-laundering and terrorist-financing risks (FATF 2025; FATF 2026). For a central bank, the migration of similar activity to a CBDC deployed on a permissionless, publicly accessible infrastructure could raise reputational concerns. Unlike private issuers, central banks are guardians of monetary sovereignty and public trust; the association of sovereign money with sanctions evasion or transnational criminal finance could erode institutional legitimacy. Moreover, the visibility and immutability of public blockchains may intensify scrutiny, as illicit use cases would be publicly traceable and symbolically tied to the issuing authority, even where legal liability is absent. BIS policy analysis has emphasized that reputational risk is a core consideration in CBDC design, particularly in relation to operational resilience and misuse (BIS 2018). If a public-chain CBDC were perceived as facilitating illicit finance, even marginally, the reputational damage could exceed the direct financial impact, affecting trust in the currency, the central bank's regulatory credibility, and its broader policy mandate. Accordingly, lessons from stablecoin misuse underscore that AML/CFT architecture, transaction monitoring, and governance controls are not merely compliance features but central determinants of reputational risk in any public-blockchain CBDC framework.

By contrast, the extensive and well documented domestic and foreign use of physical banknotes for various illicit purposes has generated comparatively limited reputational fallout for issuing central banks. The U.S. government has repeatedly reported that bulk U.S. dollar banknotes were discovered in the possession of terrorist and insurgent groups abroad; for example, during operations in Iraq, "millions of dollars in U.S. currency" were seized from insurgent networks (U.S. Department of Defense 2003). Similarly, U.S. authorities have acknowledged that high-denomination notes circulate widely outside the United States and are frequently used in underground economies (Federal Reserve Board 2022). In Europe, law-enforcement investigations have uncovered large volumes of euro banknotes in organized crime and terrorist financing contexts, prompting policy debate over the €500 note, which the ECB acknowledged had become a "concern that this banknote could facilitate illicit activities" (ECB 2016). Yet neither the discovery of bulk cash in terrorist safe houses nor the documented role of high-denomination notes in transnational crime has materially undermined the institutional legitimacy of the Federal Reserve or the ECB. The reputational insulation of banknotes appears to derive from their longstanding status as neutral bearer instruments, their global reserve-currency function, and the absence of a direct technological architecture attributable to the issuing authority. In contrast to a CBDC deployed on a public blockchain,

where illicit transactions may be symbolically and technologically associated with contemporary design choices, the misuse of physical currency has been interpreted as an externality of cash's anonymity rather than a failure of institutional governance. This asymmetry suggests that reputational risk is not solely a function of criminal use per se, but of perceived control, and design responsibility.

This proposal should also be distinguished from the vision of a "unified ledger" advanced by the BIS (2023), in which tokenized central bank money, commercial bank deposits, and other claims would coexist on shared programmable infrastructure operated within the regulated financial system. That vision shares this paper's premise, that tokenized money benefits from common programmable rails, but differs in the sense that a unified ledger is a new, permissioned infrastructure that must be built, governed, and adopted, whereas public blockchain rails already exist, already host the dominant tokenized money in circulation, and already reach the users most exposed to currency substitution.

3. Mitigants to central banks' concerns

3.1 How should central banks cope with technical limitations and fragmentation of public blockchains?

To address chain-selection risk, central banks could adopt formalized chain admission criteria. Public blockchains differ in security guarantees, finality properties, governance stability, throughput, and compliance tooling. Major stablecoin issuers select chains conservatively, optimizing across reorganization and governance risk, validator concentration, user community and liquidity. Central banks should codify similar criteria in a published risk framework, including minimum standards for probabilistic or deterministic finality, governance transparency, operational uptime, and incident response capacity. Because these guarantees are probabilistic or economic rather than legal, the framework would also need to define, for each chain, the point at which settlement is treated as final in law. As emphasized by the Bank for International Settlements (BIS 2023), technological neutrality does not preclude infrastructural due diligence.

Moreover, the framework should assess cryptographic agility, that is, a chain's ability to migrate to new signature schemes without disrupting the system, because the digital signatures securing today's public blockchains are vulnerable to future quantum computers and payment systems are already preparing for a migration to post-quantum cryptography.[2] It should also require guaranteed transaction inclusion, since a sovereign instrument should not depend on the discretionary filtering of external validators, builders, relays, or sequencers.[3]

---

[2] BIS Innovation Hub, Project Leap: Quantum-proofing payment systems, 2025, https://www.bis.org/publ/othp107.pdf; NIST, Announcing Approval of Three Federal Information Processing Standards for Post-Quantum Cryptography, 2024, https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

[3] Wahrstatter et al., Blockchain Censorship, 2024, https://doi.org/10.1145/3589334.3645431; Offchain Labs, config-force-inclusion, Arbitrum Docs, 2026, https://docs.arbitrum.io/launch-arbitrum-chain/partials/config-force-inclusion

Privacy should be treated as one infrastructural criterion, not as a separate retail policy preference to be added later. Public blockchains make transaction data widely observable, which can be useful for auditability and illicit finance detection, but it can also expose payment information to validators, analytics firms, and other third parties. A central bank token therefore would need a privacy design that limits disclosure to what is necessary for settlement and compliance, while preserving the ability of authorized institutions to apply AML/CFT controls. Recent CBDC prototypes show that payer privacy can be designed into the architecture, for example through blind signature based eCash models, while zero knowledge-based systems show more generally that validity can be verified without revealing all transaction details.[4]

A further selection criterion concerns the unit in which users pay for use of the network. A sovereign payment instrument would be weakened if its users first had to acquire and hold a volatile private crypto asset merely to pay transaction fees. The architecture should therefore allow fees to be paid in the sovereign token, or to be sponsored by the issuer or supervised intermediaries, with the central bank controlling the economic terms of that service. So-called account abstraction and paymaster models already provide a technical pattern in which a third party can sponsor fees or permit fee payment in tokens other than the native asset.[5] For a central bank, this is not only a matter of convenience, but also of monetary sovereignty, since the use of public money should not depend on a mandatory balance in another issuer's asset.

Assessing which public blockchains are currently most suitable for issuing tokenized central bank money is a matter of choosing an execution environment that meets the security, settlement-finality, governance, resilience, compliance, and reach requirements appropriate to sovereign money. Because public blockchains are heterogeneous and evolve through external governance, central banks would need to treat chain selection as a risk decision and, consistent with stablecoin practice, retain full sovereignty over the mint/burn and redemption layer, regardless of the underlying network. The assessment below reflects the state of these networks as of mid-2026; specific networks are illustrative, not prescriptive.

A first, conservative candidate is Ethereum mainnet (and, increasingly, its Layer-2 rollups). Ethereum offers the deepest smart-contract ecosystem and a relatively mature security track record, while its proof-of-stake finality mechanism uses validator checkpoints to provide economically backed finality under defined assumptions (Ethereum Foundation 2025). However, Ethereum mainnet is often operationally unattractive for high-frequency retail payments because of fee variability and throughput constraints; practical payment-grade scalability is therefore commonly sought via rollups that "inherit" Ethereum security while offering lower fees and higher throughput (Arbitrum Foundation 2026). This "Ethereum + L2" path would mirror the stablecoin industry's trajectory: Circle reports USDC as natively supported across a large multi-chain footprint and explicitly markets interoperability as a core design goal, including issuer-controlled cross-chain transfer mechanisms (Circle 2026a; Circle 2026b). For a central bank, the major advantage of

[4] Bank for International Settlements, Project Tourbillon: Exploring privacy, security and scalability for CBDCs, 2023, https://www.bis.org/publ/othp80.pdf; Ben-Sasson et al., Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014, https://doi.org/10.1109/SP.2014.36

[5] Ethereum Improvement Proposals, ERC-4337: Account Abstraction Using Alt Mempool, 2023, https://eips.ethereum.org/EIPS/eip-4337; ERC-4337 Documentation, Paymasters, 2026, https://docs.erc4337.io/paymasters/index.html

the Ethereum rollup ecosystem is that it enables segmented performance tiers (high security on L1, higher efficiency on L2) while preserving a coherent developer and liquidity base; the main disadvantages are added architectural complexity, sequencer/governance dependencies at L2, and the need to define legally robust settlement finality standards across layers.

A second candidate is Solana, which prioritizes high throughput and low fees and has gained increasing traction for stablecoin settlement in payment contexts. Visa, for example, has publicly expanded stablecoin settlement capabilities to Solana, underscoring its perceived operational performance for payments use cases (Visa 2023). The principal advantage of Solana for a retail-payments-oriented sovereign token would be efficiency (low transaction costs, fast confirmations); the main drawbacks, from a central bank's perspective, are the stronger dependence on a specific network design and governance community, operational sensitivity to network incidents (even if improving), and the concentration risks that some analysts associate with high-performance monolithic chains. In other words, Solana can be attractive for payments throughput but may require more conservative contingency planning and "circuit-breaker" issuance policies than a central bank would need on a slower, more conservative base layer.

A third family of options consists of EVM (Ethereum Virtual Machine)-compatible alternative Layer-1s such as Avalanche and Polygon PoS. Their main appeal is a combination of smart-contract compatibility with materially lower fees and faster settlement than Ethereum mainnet, and they host meaningful stablecoin activity (Haidar 2026; Koch-Gallup 2026). For a central bank, these chains could provide an attractive cost/performance envelope and leverage the EVM tooling stack. The corresponding trade-offs are governance and upgrade risk (rules set externally), varying degrees of decentralization, and potentially thinner "blue-chip" liquidity than Ethereum, factors that matter if tokenized central bank money is expected to become a settlement asset for tokenized securities and multi-asset applications (BIS 2023).

A fourth option is Tron, which has become a major settlement network for USDT and other stablecoin flows. Recent market reporting indicates that Tron accounts for a substantial share of stablecoin transfer activity and supply, illustrating how low transaction costs, broad distribution, and ease of use can support adoption. These features may be especially relevant in emerging-market corridors where currency substitution is more acute. From a central bank perspective, however, the composition of network activity, public perceptions of the ecosystem, and associated compliance considerations would still need to be assessed carefully. A sovereign issuer would therefore need to weigh Tron's demonstrated reach and accessibility alongside these considerations.

A fifth, rapidly evolving family consists of payment- and stablecoin-oriented chains such as Tempo, Arc, Plasma, and Stable (StableChain), which are explicitly designed for high-volume, low-cost money movement. Their emergence underscores both the pace of change in this segment and the value of optionality in chain selection. For a central bank, the principal caveat is that several of these networks are closely affiliated with private payment or stablecoin firms and remain early in their decentralization and operational track record; issuing on such rails could reproduce the dependence on private payment infrastructure that sovereign issuance seeks to reduce, and would therefore require particularly strict application of the admission criteria above.

An important lesson from stablecoins is that "issuing on a chain" must mean native issuance under issuer control, not reliance on third-party wrappers (tokenized representations of assets that exist on another chain) or unsanctioned bridges. The bridge layer has repeatedly been a locus of fragility, and the BIS stresses that multi-ledger ecosystems require robust interoperability arrangements and governance to avoid new vulnerabilities (BIS 2023). A central bank should therefore (i) recognize only canonical, natively issued supply per chain; (ii) use only issuer-controlled burn-and-mint mechanisms for cross-chain portability (akin in concept to issuer-led interoperability tooling marketed in stablecoin ecosystems); and (iii) maintain clear contingency powers to pause issuance on a chain where governance or security conditions deteriorate (Federal Reserve Board 2022; Circle 2026a).

In sum, no public blockchain currently dominates across all dimensions relevant to sovereign money. A pragmatic "current best fit" for many central banks would be an Ethereum-anchored approach, using Ethereum mainnet for maximum settlement assurance and one or several major rollups for efficiency, because it combines mature security dynamics, deep integration into tokenized asset markets, and a proven stablecoin interoperability playbook (Ethereum Foundation 2025; Arbitrum Foundation 2026; Circle 2026b). For high-throughput retail use cases, a selective additional issuance on a performance-oriented chain or specific stablecoin oriented chain could be of interest, provided issuance sovereignty, safe supply accounting, and issuer-controlled cross-chain mechanisms are maintained (Visa 2023; Visa 2025). If mere user adoption would be the key driver, Tron might be difficult to pass over.

Ultimately, chain choice decisions of central banks should be a risk-managed portfolio decision, not a singular bet on one chain: central banks can reduce dependency and fragmentation risks by issuing natively on a small, vetted set of chains, strictly limiting third-party bridging, and treating interoperability as a controlled extension of the issuance function rather than an external add-on (BIS 2023; Federal Reserve Board 2022).

3.2 How should central banks address safety and operational risks associated with public blockchain?

The tokenization of central bank money on public blockchains entails operational risks that require mitigation measures exceeding those typically applied by private stablecoin issuers. Given the systemic importance of sovereign money, risk controls must be formalized, transparent, and legally anchored.

First, to safeguard monetary sovereignty, central banks must retain (i) exclusive control over minting and redemption**.** Public blockchain governance must not be mixed with issuance authority. All token creation and destruction should occur through centrally controlled contracts, with legally enforceable redemption of rights. This ensures balance sheet integrity irrespective of the underlying settlement layer. (ii) To prevent supply fragmentation, central banks must define a canonical issuance model. Only natively issued tokens and issuer-controlled burn-and-mint interoperability mechanisms should be recognized as official supply. Third-party wrapped or bridged versions should neither be redeemable nor treated as equivalent claims. This minimizes contagion from bridge failures and preserves the integrity of the issuance. (iii) To mitigate interoperability vulnerabilities, central banks should avoid reliance on unsanctioned bridges. Where cross-chain functionality is required, it should be implemented through sovereign-controlled mechanisms, combined with contract-level safeguards and risk-based address controls (BIS 2023).

Exclusive issuer control is credible only if the keys conferring minting, redemption, pause, and compliance powers are governed as critical central bank infrastructure. The relevant benchmark should not be a single private key in cold storage, but a layered control model using threshold or multi-party computation (MPC)-based signing, hardware protected key material where appropriate, role separation, quorum approval, monitored policy engines, tested recovery procedures, and regular key rotation. The US National Institute of Standards and Technology (NIST) work on threshold schemes supports the use of distributed cryptographic control to reduce single point compromise of secret keys, while hardware security modules (HSM) remain the established protection model for high assurance key management.[6] Newer architectures should also be reviewed and, where they add value, used to extend this model rather than replace it, for example by keeping signing keys permanently offline or by combining hardware isolation with threshold approval. The same applies to compliance keys, since a key that can suspend transfers or change a permission list is also an attack surface. Such roles should therefore be separated from ordinary operational signing, subject to higher quorum requirements, protected by time delays where immediate action is not required, and covered by an emergency path for narrowly defined incidents. Commercially available institutional custody architectures show that these controls are already used in regulated digital asset operations, although a central bank would need to specify them as public infrastructure requirements rather than as vendor features.[7]

A distinction should be drawn between issuer-level controls and network-level control. Freezing or blocking functionality can be embedded at the token-contract level even on highly decentralized public chains. By contrast, chain-level enforcement, transaction ordering, or transaction-filtering capabilities depend on the governance and architecture of the underlying network.

Second, smart contract risk should be treated as a separate operational risk, not only as a component of chain selection. A central bank token contract would define the monetary claim, the authorized issuance path, the redemption of mechanics, and the exceptional intervention powers, so a software defect could become a monetary and legal event. Formal specification, formal verification of critical invariants, independent audits, public test deployments, and vulnerability disclosure processes would therefore be part of the minimum assurance package. Research on smart contract security identifies formal analysis and verification as important mitigation techniques, while technical documentation in the public blockchain ecosystem treats formal verification and security review as standard assurance methods for high value contracts.[8] At the same time, complete immutability is not always desirable for public money, because legal requirements, security conditions, and protocol environments may change. The more

[6] NIST, First Call for Multi-Party Threshold Schemes, NIST IR 8214C, 2026, https://csrc.nist.gov/pubs/ir/8214/c/final; NIST, Hardware Security Module HSM, CSRC Glossary, 2026, https://csrc.nist.gov/glossary/term/hardware_security_module_hsm

[7] IBM, IBM Announces Digital Asset Haven, 2025, https://www.prnewswire.com/news-releases/ibm-announces-new-platform-for-financial-institutions-and-regulated-enterprises-entering-the-digital-asset-economy-302594751.html; Ledger Enterprise, Institutional Digital Asset Platform, 2026, https://enterprise.ledger.com/; EY and Fireblocks, Digital Asset Custody and Transaction Processing Leading Practices Using Fireblocks' MPC Solution, 2025, https://www.fireblocks.com/report/digital-asset-custody-and-transaction-processing-leading-practices-using-fireblocks-mpc-solution; Taurus, What should a bank choose between HSM, MPC and TSS for digital asset custody?, 2021, https://www.taurushq.com/blog/what-should-a-bank-choose-between-tss-mpc-and-hsm-for-digital-asset-custody/

[8] Ivanov et al., Security Threat Mitigation for Smart Contracts: A Comprehensive Survey, 2023, https://doi.org/10.1145/3593293; Ethereum Foundation, Smart contract security, 2026, https://ethereum.org/developers/docs/smart-contracts/security/

suitable approach would be narrow upgradeability, with transparent governance, time delays for non-emergency changes, segregated emergency authority, and clear public records of contract versions.[9]

Third, to address governance and protocol risk, central banks must adopt predefined contingency frameworks. These should include issuance pause mechanisms, migration pathways, and clear legal treatment of finality in the event of contentious forks or network instability (Federal Reserve Board 2022).

Fourth, continuous supply of reconciliation and monitoring would be indispensable. On-chain balances must be matched in real time with central bank accounting systems, supported by independent auditability and statutory oversight.

Fifth, reputational risk requires a conservative deployment strategy. Phased roll-out, limited initial scope, strict interoperability discipline, and clearly articulated fallback procedures should guide implementation. These fallback procedures should be prepared and tested in advance as part of operational readiness, since private issuers have suspended and, in some cases, recovered assets in coordination with law enforcement, interventions comparable to account freezes under court order in conventional finance.[10] The objective is not maximal decentralization, but maximal reliability.

In sum: operational risk in public-blockchain tokenization is manageable, provided issuance control, canonical supply definition, interoperability governance, monitoring, and contingency planning are embedded ex ante into system design. Stablecoin practice offers useful precedents, but central banks can elevate these safeguards to a higher standard of accountability and transparency.

3.3 How to prevent that tokenized CBDC creates financial stability risks?

The lessons from the extensive discussions on retail CBDC over the last ten years could be the following: the appropriate policy stance should be one of preparedness rather than premature restriction. It is enough to have potential tools to restrict total volumes under some possible long-term future scenario in which success of a new form of central bank money would really be exorbitant. The central bank should not concede ex ante to apply restrictive measures on public money before there is any need for it, while there is no comparable restrictive measure on any form of private money. A large demand for on-chain central bank money tokens would first be a success of the project and be positive in view of the declining use of banknotes. It would mean preserving seigniorage income which should be much appreciated in a world of high and growing fiscal pressures. It would also mean that the other public policy objectives that have been translated into the design of the on-chain central bank money would be effective at larger scale (e.g. the lower tolerance for illicit payments, compared to some stablecoins).

---

[9] Security Alliance, Secure Multisig Best Practices, 2026, https://frameworks.securityalliance.org/wallet-security/secure-multisig-best-practices/; OpenZeppelin, Access Control, 2026, https://docs.openzeppelin.com/contracts/4.x/access-control

[10] Elliptic, KuCoin Thief Sells Out Millions in Crypto Tokens on Decentralized Exchanges, 2020, https://www.elliptic.co/blog/kucoin-thief-sells-out-millions-in-crypto-tokens-on-decentralized-exchanges; Chainalysis, The Landscape of Seizable Crypto Assets in 2025, 2025, https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/

Second, if really the demand for central bank money tokens would exceed expectations, a mitigant could be the readiness of the central bank to address a significant increase of its monetary liabilities through asset purchase programs, such as to avoid an increase of banks' structural dependence on central bank credit. This can take both the form of domestic outright portfolios (which does not necessarily be biased to short term or sovereign bond issuers) and increased foreign reserves. The latter makes sense if the central bank money token is to a significant degree held abroad: then the purchase of additional foreign assets neutralizes the effect of capital inflows associated with circulation of central bank money abroad on FX rates.

Whether and to what extent a central bank makes use of such balance sheet offsets is ultimately a matter of its own operating framework and institutional preferences. Views on the appropriate scale and composition of central bank asset holdings differ across jurisdictions and traditions. In some settings, for instance in monetary unions or in economies with deep sovereign-bond markets, these questions are the subject of ongoing debate. In the jurisdictions on which this paper primarily focuses, they tend to arise in a less pronounced form. There is no need to prejudge here these choices, which remain for each central bank to make within its own mandate, but to note that the balance-sheet tools discussed above are available.

The following sectoral financial accounts show the mitigants available to the central bank that can effectively prevent an increased dependence of banks on central bank credit. We limit ourselves to the one-country case, but the two-country case can easily be constructed in analogy to Bindseil (2025). The general issue of how CBDC can help prevent a decline in the circulation of public money and thereby preserve sovereignty and seigniorage income is addressed in Annex 1. We assume that households and NBFIs (which we treat together as one sector) finance CBDC purchases in two ways:

- a share β [0,1] by reducing sight deposits with banks,
- a share 1-β by reducing banknotes.

We moreover assume that the central bank can "re-invest" the increase of its monetary liabilities (which will amount to β*CBDC) as follows:

- A share α [0,1] is held in the form of increased credit to banks.
- A share δ [0,1- α] is held in the form of securities purchased from banks
- A share **(1- α - δ)** is held in the form of securities purchased from households/NBFIs.

The choice of δ and therefore of (1- α - δ) is not perfectly in the hands of the central bank (while α is), since it depends on relative supply elasticities between banks and households/NBFIs. The central bank could somewhat influence it by specifically buying bonds which are more in the hands of one of the two, or where it knows that the supply elasticities are very different. Figure 1 shows the relevant flows of funds.

Figure 1: Financial account representation of flows of funds from stablecoin-creation, single country case

Households and NBFIs			
Sight deposits	**$-\beta + (1-\alpha-\delta)$ CBDC**	**Other net liabilities**	
CeBSC	**CBDC**		
Banknotes	**$-(1-\beta)$ CBDC**		
Bonds	**$-(1-\alpha-\delta)$ CBDC**		
Commercial Banks			
Bonds	**$-\delta\beta$ CBDC**	**Sight deposits.**	**$-\beta + (1-\alpha-\delta)$ CBDC**
		Central bank credit	**$\alpha\beta$ CBDC**
Central Bank			
Credit to banks	**$\alpha\beta$ CBDC**	**Banknotes issued**	**$-(1-\beta)$ CBDC**
Bonds	**$(1-\alpha)\beta$ CBDC**	**CBDC**	**CBDC**

Figure 1 illustrates that, under suitable operating-framework conditions, the central bank has balance-sheet tools that can mitigate the impact of CBDC demand on bank funding. It can choose $\alpha=0$ and on top aim at buying securities from households /NBFIs. It is also in the hands of banks to impact on δ by choosing their supply elasticity for bonds. Therefore, provided that the central bank essentially sets $\alpha=0$, even large CBDC volumes do not impact aggregate sectoral accounts. Of course, what was previously granular household deposits might now be partially less stable and/or more expensive deposits of NBFIs. But this can also occur without any CBDC issuance, since households can change the way they want to hold their liquid reserves (e.g. in the form of stablecoins, money market funds, etc.), which can equally reduce the amount of granular, cheap, stable deposits which support the business model of banks.

For as long as nominal short-term rates do not fall into low or negative territory (as they did between 2015 and 2021 in Europe and in Japan for more than two decades), i.e. as long as the absence of remuneration constrains the attractiveness of CBDC as store of value, no additional precautions seem to be needed. If policy rates were instead to approach zero or become negative, (negative) remuneration tools could become relevant to prevent tokenized CBDC from becoming a disproportionate store of value. Such tools should be exceptional safeguards rather than default design constraints, with the central bank committing to use them only under pre-defined conditions. For emerging market and developing economies (EMDEs) zero or very low nominal interest rates are the absolute exception, and therefore non-remuneration of CBDC should almost always be sufficient to prevent a disproportionate reliance on CBDC as store of value.

3.4 How to address reputation risks associated with illicit usage of CBDCs on public blockchain?

As discussed in more detail in section 2.4, the prospect of issuing central bank tokens on public blockchains raises questions regarding the prevention of illicit use, particularly money laundering, terrorist financing, sanctions evasion, and large-scale fraud. While it is frequently argued that public blockchains increase traceability relative to cash, central banks would nevertheless face heightened reputational and legal

expectations compared to private issuers. Physical cash is widely used for tax evasion and criminal activities, yet this fact has not fundamentally undermined the legitimacy of banknotes. Central banks traditionally defer to legislatures in setting up cash usage thresholds and reporting requirements. However, sovereign digital tokens circulating on transparent public infrastructures would likely attract far greater scrutiny, necessitating a more formalized and proactive compliance architecture.

Recent experience with stablecoins provides a relevant template for how central banks can address such challenges. Major issuers such as Circle (USDC) combine ex ante controls at issuance and redemption with continuous transaction monitoring, blacklist functionality, and the technical capacity to freeze tokens at the smart-contract level. Centralized stablecoin contracts routinely incorporate administrative keys enabling asset freezing and address blacklisting (Makarov and Schoar 2022; BIS 2023). Central banks could replicate, and formalize, this architecture by restricting issuance and redemption of their tokens to supervised credit institutions and regulated payment service providers, embedding programmable compliance hooks into token contracts, and integrating state-of-the-art blockchain analytics tools to detect suspicious flows in real time (FATF 2026). Such measures would operationalize the risk-based approach endorsed by international AML/CFT standards.

Given their public mandate, central banks would likely need to go further than private issuers in institutionalizing transparency, auditability, and due process safeguards around interventions. Clear statutory bases for freezing and blocking powers, predefined maximum durations for precautionary freezes pending law-enforcement action, and ex post judicial review mechanisms would be essential to safeguard proportionality. Address-level restrictions could be calibrated to distinguish between temporary suspension of suspect balances and permanent exclusion from the ecosystem. A tiered-access design could further reconcile financial integrity with privacy: low-value wallets might be permitted with simplified due diligence or limited anonymity, subject to transaction and holding caps, while higher-value accounts would require full customer identification, consistent with FATF guidance on digital identity and travel rule implementation (FATF 2025; FATF 2026). If intervention were too discretionary or too easy to activate, the instrument could become less attractive than cash and stablecoins. The design challenge is therefore to combine credible AML/CFT safeguards with clear limits of intervention, procedures, and accountability mechanisms.

These safeguards, however, presuppose that they can in fact be enforced on the underlying infrastructure. A related question is whether the central bank's legal and operational rules can be made effective at the level of the chain itself. On a public blockchain, validation, transaction ordering, and protocol governance are not operated by the issuer and would normally lie largely outside its jurisdiction. A central bank issuing on such infrastructure would therefore need to ensure, through the contract level controls and chain selection criteria discussed above, that the relevant rules can take effect on chain, and to identify mitigants where this cannot be ensured fully. Otherwise, the instrument could create a reliance on external payment infrastructures, analogous in policy terms to the dependence on international card schemes and global big tech providers in retail payments that European authorities have sought to reduce in the interest of

strategic autonomy.[11] The operating framework would thus be an instrument for preserving monetary sovereignty on infrastructure that the issuer does not itself operate.

Fungibility also requires a legal answer, not only a technical one. Banknotes have historically been able to function as money because a good faith recipient can normally acquire clean title, a principle associated with the Miller v Race line of cases and reflected in modern legal systems through special rules for money and bearer instruments.[12] If a central bank token can carry a permanent taint through transaction history, users may be reluctant to accept it from unknown counterparties, even where they have no connection to an earlier unlawful transaction. The legislature would therefore need to clarify how traditional good faith acquisition principles apply to tokenized central bank money, including whether restrictions should operate prospectively and what effect they have on subsequent recipients. This is not primarily a demand that the central bank compensate for all false positives, but a question of the legal character of the instrument as money. Without such clarification, a technically traceable token could become less fungible than banknotes and therefore less suitable as public money.

A general limitation must be acknowledged: while issuance and redemption can be confined to supervised institutions, peer-to-peer transfers between self-hosted wallets on a public chain are not intermediated, so per-transaction due diligence and holding caps are enforceable primarily at regulated on- and off-ramps and at the contract level (through freezing and blacklisting), rather than continuously along the transfer path. This mirrors the "unhosted wallet" challenge already familiar with stablecoin regulation (FATF 2026) and implies that compliance assurance rests on issuance/redemption gating, contract-level controls, and analytics, not on intermediating every transfer. Cross border circulation adds a further coordination problem, since a token deliberately designed to circulate abroad may face conflicting legal instructions across jurisdictions, for example where one authority requires restriction while another limits compliance with extraterritorial measures.[13]

Against this background, the concrete control toolkit an issuer could deploy would combine several elements, reflecting the enforceability considerations set out above and their residual limits at the self-hosted-wallet and cross-border level. Additional controls could include (i) mandatory whitelisting of smart contracts interacting with the token; (ii) restrictions on interoperability with higher-risk bridge protocols; (iii) automated reporting triggers for suspicious transaction patterns; and (iv) redemption gating mechanisms preventing conversion into reserve assets where compliance flags are active. The "enforcement-privacy trade-off" must be explicitly acknowledged, and it should be explained why central banks put quite some emphasis on enforcement. Stronger monitoring and intervention capabilities may reduce illicit-use risks, but they can also weaken the cash-like qualities that make public money broadly

[11] European Central Bank, The Eurosystem's retail payments strategy: priorities for 2024 and beyond, 2023, https://www.ecb.europa.eu/pub/pdf/other/ecb.eurosystemretailpaymentsstrategy~5a74eb9ac1.en.pdf
[12] Fox, Bona Fide Purchase and the Currency of Money, 1996, https://ecashact.us/files/Fox1996.pdf; Bundesministerium der Justiz, § 935 Abs. 2 BGB (Ausnahme für Geld und Inhaberpapiere vom Ausschluss des gutgläubigen Erwerbs), https://www.gesetze-im-internet.de/bgb/__935.html
[13] European Commission, Extraterritoriality Blocking Statute, 2026, https://finance.ec.europa.eu/eu-and-world/open-strategic-autonomy/extraterritoriality-blocking-statute_en; FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021, https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

acceptable. The design should therefore acknowledge the tension between financial integrity, privacy, and user autonomy. By embedding compliance into token design while ensuring procedural safeguards and proportionality, central banks could issue public-blockchain tokens that preserve technological advantages without compromising their reputation.

As a final remark, it is acknowledged that a further tension exists between, on the one hand, the proposed efforts of central banks issuing CBDC on-chain to ensure compliance and to avoid the use of public money for on-chain illicit activity, and, on the other hand, the observation that the reputational insulation of banknotes and their status as neutral bearer instruments can be attributed precisely to the absence of a direct technological monitoring architecture attributable to the issuer. In other words, the explicit effort and ambition to prevent the use of on-chain CBDC for illicit activities (both for objective public good reasons and for narrower reputational risk reasons) could in net terms increase reputational risks, as critics of the central bank could argue that "the central bank should have known," or that "the central bank spent considerable public money on technical prevention, yet still failed to prevent cases X and Y." Anticipating this issue, the central bank should refrain from claiming ex ante that it can prevent illicit use with certainty, and should prepare a communication strategy to respond to critics when illicit usage is detected ex post. Minimizing investment in preventing the illicit use of on-chain CBDC, so as to achieve a perception equivalent to that of banknotes (namely that the central bank has nothing to do with such abuses of central bank money and could not, in any case, know anything about them) does not appear to be a viable alternative. First, it would be inconsistent with the regulatory pressure on stablecoin issuers to make efforts to prevent illicit use; second, it would betray the public good objectives of central banking.

3.5 Alternative: specifically licensed and fully central bank money backed stablecoins

One way to shield the central bank from operational and reputational risk, while potentially coming close to achieving the same benefits as genuine CBDC on chain, is to establish a framework for stablecoins that would come close to having the same properties as CBDC, even if, strictly speaking, they would remain private money. Beyond compliance with the applicable domestic framework for stablecoins (e.g. MiCAR), these stablecoins would need to (i) fulfil additional minimum criteria established by the central bank, (ii) be subject to a specific license, and (iii) be fully backed with central bank money as reserve assets. We call these “central bank stablecoins” (such constructs were also called “synthetic CBDC”, but strictly speaking they are stablecoins and should be designated accordingly). The Bank of England (2023) had expressed a preference to regulate UK stablecoins in such a way that they must hold all their reserves with the Bank of England, and that these reserves would be remunerated at zero.[14] We propose to consider the following variant of Bank of England (2023):

i. Full backing in CeBM (while not mandatory per law for all stablecoins) is a key defining criterion for a special “central bank stablecoin” (CeBSC) license.

[14] In Bank of England (2026), systemic stablecoin issuers are permitted to hold 70% of backing assets in short-term UK government debt securities and must hold the remaining 30% as unremunerated central bank deposits; a temporary issuance guardrail of £40 billion applies to each systemic stablecoin.

ii. The reserve is remunerated, and the rate of remuneration varies normally in parallel with the level of the central bank policy rate. The spread between the policy rate and the remuneration rate depends on several considerations: (i) being attractive enough to support the CeBSC business model; (ii) a fair sharing of seigniorage income between the central bank and the licensed CeBSC issuers; (iii) the costs of the activities left to the SC issuer and the costs of compliance with the specific minimum standards for CeBSC issuers.

iii. CeBSC could be allowed to remunerate their tokens (in the same way as banks are allowed to remunerate sight deposits), but not necessarily. If so, the remuneration offered by the central bank for the reserve of the CeBSC provides a natural upper constraint of the remuneration that the issuers can offer to holders of the CeBSC, and thereby can also become an instrument to protect the business model of banks, if desired.

iv. CeBSC would be licensed under an agreement which would foresee a number of mandatory minimum features, such as strong, state of the art AML/CFT controls; eligible blockchains and bridging practices; blocking capabilities, transparency requirements; etc..

v. Technical requirements ensuring a certain degree of interoperability.

A low number of licenses would be granted, such as to avoid excessive fragmentation, while ensuring competition. The selection of these could be done within a tender procedure, on the basis of the quality scoring of applications (e.g. the three which would reach the highest quality and credibility scores could be selected).

In September 2025, the National Bank of Kazakhstan launched a tenge-denominated stablecoin on a public blockchain (Solana) within its regulatory sandbox, issued by a licensed private entity, an arrangement closely corresponding to the CeBSC model described here (National Bank of Kazakhstan 2025). Related experiments include Palau's government-backed stablecoin on public infrastructure and the state of Wyoming's WYST token deployed across several public networks. None of these is central bank money in the legal sense.

4. Conclusions

This paper revisits the recently neglected option of issuing central bank money directly on public blockchains. While CBDC debates have focused on centrally managed ledger systems, private stablecoins have rapidly expanded on open networks. Public blockchains offer 24/7 global infrastructure, composability, and smart-contract functionality. Tokenizing central bank money into public blockchains would not substitute banknotes, nor for the current efforts to launch CBDC as POI instrument but would complement both. For many jurisdictions, especially smaller or emerging-market economies, a broad proprietary CBDC infrastructure may be costly relative to its likely benefits; a lighter model on public blockchain rails may provide a more proportionate path. Central banks' concerns on tokenized central bank money on public blockchain (technical fragmentation, governance dependence, operational risk, financial stability effects, and reputational exposure to illicit use) are real but manageable. Stablecoin practice demonstrates that issuer control over minting, redemption, freezing, and compliance can coexist with public-chain deployment. Chain-selection risk can be mitigated through formal admission criteria,

canonical issuance models, and sovereign-controlled interoperability. Operational resilience requires clear governance frameworks, contingency mechanisms, and real-time supply reconciliation. Financial stability risks from potential deposit substitution can be contained through non-remuneration and be neutralized through asset purchase policies (and, if necessary, in the context of very low or zero market interest rates, through negative remuneration tools). Illicit-use concerns should be addressed through embedded AML/CFT architecture, programmable compliance, and technically effective and legally anchored intervention powers. Compared to private stablecoins, central banks are uniquely positioned to combine public policy objectives with blockchain functionality. An alternative model, namely fully central-bank-backed licensed stablecoins, may offer a transitional, complementary or alternative solution.

Payment instruments rely on networks and two-sided markets, and therefore payment instrument choices of societies exhibit concentration (and thus market power of successful private firms), path dependencies, and the stability of possibly inferior equilibria. This implies that launching a new payment instrument is challenging and requires high initial investments, including into deployment, and thus financial risks. However, public money has several privileges in this respect: First, legislation can declare some form of legal tender status. Second, as store of value, public money is free of any credit risk. Generally, governments are widely trusted as issuers, and therefore merchants will be more willing to invest in and promote the use of public money. Of course, these attributes cannot address the case of a government that is not trusted or a currency that suffers from very high inflation rates (and if dollarization is an option). In addition, the deployment strategy of a new form of public money could include: Using public-sector disbursements to support adoption where legally and operationally appropriate, provided that users retain access to alternative payment channels; Making the use free, including for merchants (since the costs of the instrument can be covered by seigniorage income); Making all necessary investments into achieving the highest degree of convenience of the payment instruments relying on CBDC; Undertaking a marketing campaign with reliance on media and the public sector communication outlets, emphasizing the benefits of the new solution; Offering remuneration, at least temporarily. Even a small remuneration would emphasize and draws attention to the difference and progress compared to banknotes. The same infrastructure may also become relevant for AI and agentic commerce, where autonomous software agents increasingly initiate automated payments and require programmable settlement. A CBDC issued on public blockchain rails would help ensure that the national currency remains usable not only in today's retail payments, but also in this emerging world of agentic economic activity.

Central banks should not retreat from innovation but strategically engage with public blockchain infrastructure. Issuing sovereign money on public chains could strengthen monetary sovereignty, generate seigniorage, and ultimately also support tokenized financial markets. The question is not whether public blockchains will host money, but whether central banks will participate in shaping that monetary future for the benefits of society and their monetary sovereignty.

Literature

Arbitrum Foundation. 2026. “Inside Arbitrum Nitro.” Arbitrum Docs. Accessed August 1, 2026. https://docs.arbitrum.io/how-arbitrum-works/a-gentle-introduction.

Ashraf Khan and Majid Malaika (2021), Central Bank Risk Management, Fintech, and Cybersecurity, WP/21/105

Bank of England. 2023. “Regulatory Regime for Systemic Payment Systems Using Stablecoins and Related Service Providers: Discussion Paper.” 6 November 2023. https://www.bankofengland.co.uk/paper/2023/dp/regulatory-regime-for-systemic-payment-systems-using-stablecoins-and-related-service-providers.

Bank of England. 2026. “Sterling-Denominated Systemic Stablecoins.” Policy Statement, 22 June 2026. https://www.bankofengland.co.uk/paper/2026/ps/sterling-denominated-systemic-stablecoin.

Bank for International Settlements (BIS). 2018. Central Bank Digital Currencies. CPMI Papers No. 174. Basel: BIS.

Bank for International Settlements (BIS). 2022. Annual Economic Report 2022: Chapter III—The Future Monetary System. Basel: BIS.

Bank for International Settlements (BIS). 2023. Blueprint for the Future Monetary System: Improving the Old, Enabling the New. Basel: BIS.

Barrdear, J., and Kumhof, M. (2021) “The Macroeconomics of Central Bank Issued Digital Currencies,” Journal of Economic Dynamics & Control, 142:1-24. (Initially published as Bank of England Working Paper No. 605 in 2016).

Bindseil, U. and R. Senner (2023) Macroeconomic modelling of CBDC: a critical review, ECB WPS 2978

Bindseil, U. (2025), “Regulatory responses to the financial stability implications of stablecoins”, SAFE Working Paper 470.

Buterin, Vitalik (2015): On Public and Private Blockchains, Updated Mar 6, 2023, https://www.coindesk.com/markets/2015/08/07/vitalik-buterin-on-public-and-private-blockchains.

Buterin, Vitalik (2017), “The Meaning of Decentralization,” The Medium, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274;

Buterin, Vitalik (2021), The Limits to Blockchain Scalability, https://vitalik.eth.limo/general/2021/05/23/scaling.html

Chainalysis. 2026. The 2026 Crypto Crime Report. New York: Chainalysis.

Circle. 2026a. “Multi-Chain USDC.” Circle.

Circle. 2026b. “Building the Internet Financial System: Circle’s Product Vision for 2026.” Circle Blog, January 29, 2026.

Consensys (2020), “Central banks and the future of digital money An overview and proposal for central bank digital currency on the Ethereum blockchain”, Davos, 20 January 2020.

Ethereum Foundation. 2025. “Proof-of-Stake (PoS).” Ethereum Developer Documentation. Accessed August 1, 2026. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

European Central Bank (ECB). 2016. “ECB Ends Production and Issuance of €500 Banknote.” Press Release, 4 May 2016. https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html.

Federal Reserve Board. 2022. “Security Considerations for a Central Bank Digital Currency.” FEDS Notes, February 3, 2022. Washington, DC: Board of Governors of the Federal Reserve System.

Citi Global Perspectives & Solutions. 2025. The Future of Money: Stablecoins and Digital Assets 2025 Outlook. New York: Citigroup.

Financial Action Task Force (FATF). 2025. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris: FATF.

Financial Action Task Force (FATF). 2026. “Targeted Report on Stablecoins and Unhosted Wallets Peer-to-Peer Transactions”. Paris: FATF.

Haidar, Y. 2026. “State of Avalanche Q4 2025.” Messari, 29 January 2026. https://messari.io/report/state-of-avalanche-q4-2025.

Koch-Gallup, J. 2026. “State of Polygon Q4 2025.” Messari, 4 February 2026. https://messari.io/report/state-of-polygon-q4-2025.

Makarov, Igor, and Antoinette Schoar. 2022. “Cryptocurrencies and Decentralized Finance.” Brookings Papers on Economic Activity (Fall 2022): 141–215.

National Bank of Kazakhstan (2025), “First tenge-denominated stablecoin launched in the National Bank’s regulatory sandbox”, press release, September 2025.

Nyffenegger Remo (2024), A proposal for a layer-2 CBDC on a rollup, Digital Finance, 6, 543–571.

Tarik Hansen and Katya Delak (2022), “Security Considerations for a Central Bank Digital Currency”, FEDS notes, 3 February 2022.

TRM Labs. 2026. 2026 Crypto Crime Report. San Francisco: TRM Labs.

Visa. 2023. “Visa Expands Stablecoin Settlement Capabilities to Merchant Acquirers.” Visa Press Release, 5 September 2023. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.19881.html.

Visa. 2025. “Visa Launches Stablecoin Settlement in the United States, Marking a Breakthrough for Stablecoin Integration.” Visa Press Release, December 16, 2025.

Zhang, Tao and Zhigang Huang (2022), Blockchain and central bank digital currency, ICT Express, 8/7), 264-270.

Annex 1: How payment innovation undermines seigniorage income and how CBDC on public blockchain can contribute to addressing this risk.

This annex briefly explains how reliance on conventional private means of payment and on domestic (country B) and foreign (country A) stablecoins undermines seigniorage income in country B and thereby monetary sovereignty and how CBDC can contribute to regain seigniorage income. We can parametrize this problem as follows:

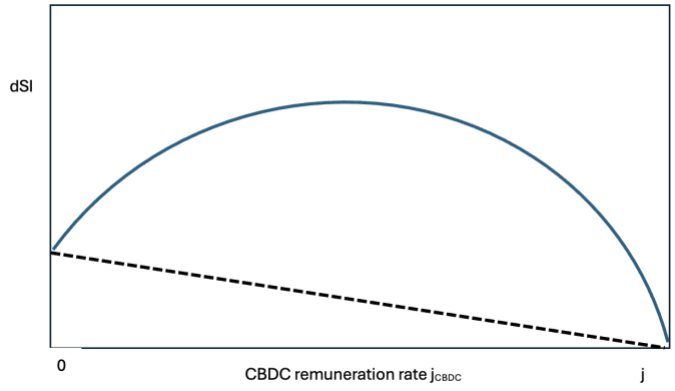
- Substitution in country B of banknotes by deposits with banks because of the declining use of banknotes in payments: Q
- Circulation of foreign stablecoins (issued in country A, circulating in country B): S_{AB}
- Circulation of domestic stablecoins (issued in country B, circulating in country B): S_{BB}
- CBDC issued by central bank B: CBDC
- Households finance a share β [0,1] of their investment in new forms of money (SCs and CBDCs) by reducing sight deposits with banks and we assume for simplicity of presentation that one parameter applies equally to the two SCs and to CBDC, a share μ in [0,1-β] of their investment into new forms of money (SCs and CBDCs) is financed in the form of banknotes s, a share **(1- μ - β)** of their investment into new forms of money (SCs and CBDCs) is financed by reducing their holdings of debt instruments.
- We moreover assume that the reserve of stablecoin B is held in the following three forms: A share α [0,1] is held in the form of commercial bank deposits. A share δ [0,1- α] is held in the form of deposits with the central bank. A share **(1- α - δ)** is held in the form of bonds. In the stylized model in which we had aggregated households and NBFIs, the bonds can only come from banks.

The financial accounts below show all effects of financial innovation on the monetary base and on the banking system. If instead the central bank chooses the CeBSC model (see section 3.5), the only modification to be done above in the financial accounts representation is to replace “CBDC” by “CeBSC”.

The total change of the monetary base (or central bank money issued) is thus **dMB = -Q - μ($SC_{AB.}$+SC_{BB}) + CBDC.** The change of seigniorage income for a certain year is accordingly **dSI = E(j)*dMB**, whereby E(j) is the average remuneration rate of central bank assets matching the monetary liabilities, and assuming that CBDC is not remunerated. If the central bank does not issue CBDC, then it will certainly face a declining balance sheet and seigniorage income.

Country B (in currency B; exchange rate 1:1)	
Households, pension and investment funds, insurance companies	
Sight deposits $Q - \beta (SC_{AB.} + SC_{BB} + CBDC)$ A-SCs SC_{AB} B-SCs SC_{BB} CBDC CBDC Banknotes $-Q - \mu(SC_{AB.} + SC_{BB} + CBDC)$ Bonds $-(1-\mu-\beta)(SC_{AB.} + SC_{BB} + CBDC)$	Other net liabilities
Stablecoin issuer	
Deposits with banks. $\alpha (SC_{BB})$ Deposits with CeB $\delta (SC_{BB})$ Government bonds $(1-\alpha-\delta)(SC_{BB})$	SC issued SC_{BB}
Commercial Banks	
Bonds $(1-\mu-\beta)(SC_{AB.}+SC_{BB}+CBDC)-(1-\alpha)(SC_{BB})$	Sight deposits. $Q - \beta (SC_{AB} + SC_{BB} + CBDC)$ SC issuer deposits $\alpha (SC_{BB})$ CeB credit $-Q - \mu(SC_{AB.}+SC_{BB}) + CBDC$ A-country banks SC_{AB}
Central Bank	
Credit to banks $-Q - \mu(SC_{AB.}+SC_{BB}) + CBDC$	Banknotes issued $-Q - \mu(SC_{AB.}+SC_{BB})$ CBDC CBDC

If CBDC is remunerated, this will boost the demand for it but of course reduce at the same time the intermediation spread. Since the monetary income generated by CBDC issuance necessarily falls to zero when the remuneration rate of CBDC reaches the asset remuneration rate j, we can assume that the monetary income curve from CBDC expressed as a function of a possible remuneration of CBDC, $dSI_{CBDC} = (E(j) - j_{CBDC})*CBDC(j_{CBDC})$ has one of the shapes depicted in the following figure. The dotted line would materialize if the demand elasticity of CBDC regarding remuneration is zero. The continuous, concave curve could materialize if the demand elasticity is positive and if the initial effect of remuneration on demand overcompensates the lower intermediation spread.



When deciding whether to issue CBDC from a monetary income perspective, the central bank needs to compare the additional seigniorage income expected from CBDC to the cost of issuance. Issuance of CBDC on public blockchains would be expected to be more efficient than banknotes for issuance and handling and should therefore break even for relatively low volumes of CBDC in circulation. The investment risk could also be shared between the central bank and the technology provider, in the sense that the fixed set up costs for the technology provider are not or only partially billed to the central bank, and the central bank instead shares a part of the future CBDC related monetary income (say 5%) with the technology provider for the duration of the contract.

How can we estimate the expected circulation of CBDC? Many countries (other than the euro area and the US; who have higher values) have banknotes in circulation of around 6-8% of GDP. We could assume that this would also be the potential for CBDC, although higher numbers for CBDC in the medium to long term would also seem to be possible if CBDC is more convenient to store and use than banknotes.

The gross domestic product (GDP) of an average Latin American economy is approximately USD 200 billion, compared to USD 60 billion for Africa and USD 360 billion for south-eastern Asia. Assuming a USD 200 billion economy, an initial 2% CBDC/GDP ratio and a nominal interest rate of 5%, and unremunerated CBDC, we obtain an annual income of USD 200 million. If we assume that CBDC is remunerated at 1% and reaches 6% of GDP, then income generated is USD 480 million, etc. If central banks do not act and eventually banknotes would no longer be used and vanish, then this loss would mean for an average USD 200 billion economy (with a 6% previous banknotes circulation and an interest rate of 5%) a loss of public sector income of USD 600 million. Issuance of CBDC can compensate for that partially, or, if well done and having convincing use cases and high convenience, even over-compensate.

Costs of CBDC issuance include three elements:

- Fixed costs from setting up initially the system.
- Annual fixed running costs (maintaining a team of experts, monitoring compliance issues, etc.).
- Variable cost per payment.

While the first two types of costs should be covered by the seigniorage income generated by the central bank (which will also pay service providers out of this income), the third type of costs may arise to users when making payments on public blockchain. It must be ensured that these costs should be very low (say not more than in the order of magnitude of a cent), so that they are practically negligible from the perspective of users and merchants. In any case, these costs would be much lower than the ones faced with traditional private electronic payments solutions.