SUERF
The European Money and Finance Forum

SUERF Policy Note
No 436, November 2026

Wholesale CBDC on public blockchains: What can central banks control?






Jan Camenisch | Category Labs
Julien Donnet | Taurus SA
Simon Lavater | SIX
Thomas Moser | Swiss National Bank

Keywords: Wholesale CBDC, tokenization, public blockchains, stablecoins, settlement finality, financial market infrastructure

JEL codes: E42, E58, G23, G28, O33

Abstract

Public blockchains increasingly host tokenized financial assets, but settlement on these networks relies heavily on privately issued stablecoins. Issuing wholesale CBDC (wCBDC) on public blockchains could enable these assets to settle in central bank money. This note examines the safeguards and trade-offs involved. We distinguish three levels of control: the monetary instrument, the applications that use it, and the underlying network. Central banks can retain control over the monetary instrument, but face trade-offs between openness and control at the application level and cannot control the underlying network. Additional safeguards can mitigate some of these dependencies but often require governed components that limit the benefits of permissionless infrastructure. The choice of infrastructure is therefore a spectrum rather than a binary one. Since network dependencies cannot be eliminated, credible recovery and exit arrangements are essential.

Disclaimer: This Policy Note is based on Camenisch, Donnet, Lavater and Moser (2026), "Wholesale CBDC on Public Permissionless Blockchains: Challenges, Trade-offs, and Design Choices," SNB Economic Studies 15/2026. The views expressed are those of the authors and do not necessarily reflect those of the institutions the authors are affiliated with.

Introduction

Banks and asset managers are issuing deposit tokens, tokenized funds, and tokenized securities on public permissionless blockchains[1]. Settlement on these chains relies heavily on stablecoins, a form of private money that carries credit and liquidity risks and can deviate from par. Much of this activity resembles wholesale financial-market transactions (Schär et al. 2026), for which international standards favor settlement in central bank money. This raises the question of how central banks can make central bank money available for settlement on public chains. There are two broad approaches. The first, already available, is to synchronize the settlement of tokenized assets on public chains with payments in a real-time gross settlement (RTGS) system. The Swiss National Bank (SNB) supports this approach in Project Helvetia, and the Eurosystem's Pontes service links market DLT platforms with its RTGS system in a similar way. The second option is to issue tokenized central bank money directly on a public chain. So far, central banks have issued wholesale CBDC (wCBDC) only on permissioned platforms. However, the Eurosystem's longer-term Appia project will assess by 2028 on which infrastructures tokenized central bank money should be provided, explicitly including networks not operated by the Eurosystem (ECB 2026a, 2026b).

This note examines the safeguards needed for direct issuance of wCBDC on a public permissionless blockchain. Bindseil and Duve (2026) make a complementary case for placing central bank money on public blockchains. They emphasize the economic benefits of reusing existing networks, wallets and software, which are potentially lower infrastructure costs, faster deployment, and less vendor lock-in. Our focus is different. Whereas they consider central bank money for a broad range of uses, including retail payments, we examine its use for wholesale settlement. We focus on direct issuance on the public base layer (Layer 1) where the central bank has the least control over the infrastructureas a benchmark. This brings the operational and legal consequences of limited control over applications and network services into focus. For comparison, we use the SNB's Project Helvetia, in which wCBDC settles transactions on a regulated, permissioned platform in a live production environment.

Our central argument is that a central bank can retain authority over the monetary instrument on a public blockchain without controlling the infrastructure on which it operates. We show how control differs across the asset, application and network levels, and why efforts to recover network-level assurances produce a spectrum of designs rather than a binary choice. Because some dependencies cannot be eliminated, credible recovery and exit arrangements are a prerequisite for deployment.

Why central bank money on public blockchains?

Outstanding stablecoins total about USD 300 billion, of which around 97 percent are denominated in U.S. dollars (Adrian et al. 2025). As private money, stablecoins expose holders to issuer credit and liquidity risks, and their market prices can deviate from par. When Silicon Valley Bank failed in March 2023 while holding about 8 percent of USDC's reserves, USDC fell to around USD 0.90 in secondary markets (Du et al. 2025). None of the 68 stablecoins studied by Kosse et al. (2023) maintained its peg continuously. Such deviations weaken the singleness of money: instruments denominated in the same currency no longer reliably exchange at par (BIS 2025). Even small deviations matter for large-value settlement. A deviation of ten basis points on a USD 100 million transaction amounts to USD 100,000. International standards therefore favor central bank money for settlement: Principle 9 of the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) calls for settlement in central bank money where practical and available (CPMI-IOSCO 2012).

Tokenized deposits mitigate some of these risks but do not eliminate the need for central bank money. As claims on regulated banks, they benefit from prudential supervision and bank's access to central bank liquidity. Yet, a tokenized deposit remains a liability of the issuing bank. Transfers between customers of that bank can be recorded on its own balance sheet, but payments to customers of another bank create interbank obligations that must be settled. Even

[1] Throughout this note, we use "public blockchains" and "public chains" as shorthand for public permissionless blockchains. The two properties are distinct: "public" means that anyone can read the ledger and submit transactions, while "permissionless" means that anyone can participate in transaction validation without prior authorization.

when deposits are issued on shared blockchain infrastructure, interbank transfers therefore require a common settlement asset or an equivalent settlement arrangement. Central bank money provides a common settlement asset free of issuer credit risk and helps preserve the singleness of money across banks.

The case for wCBDC on a public chain rests on two arguments. First, as tokenized markets grow on public chains without access to central bank money, they are likely to rely increasingly on private settlement assets. Making wCBDC available on these chains would preserve central bank money as the settlement anchor. Access would remain restricted to eligible institutions, consistent with the two-tier monetary system: customers would transact through banks, which would settle interbank obligations in central bank money. Second, wCBDC could settle transactions where tokenized assets already reside. Arrangements linked to RTGS can also provide settlement in central bank money, but they require coordination between the blockchain and a separate settlement system. By contrast, when money and assets share one execution environment, both legs of a trade can execute together or not at all. The distinctive advantage is not programmability alone, which private platforms also offer, but native interaction with assets and applications on the public chain.

This benefit is greatest when independently issued assets already share a public chain. Securities from multiple issuers could settle against wCBDC without requiring every issuer to join a common private platform. Banks issuing deposit tokens on that chain could settle the resulting interbank obligations in central bank money as their customers transact. If several central banks issued wCBDC in the same environment, foreign exchange transactions could also settle atomically without a jointly operated platform, as explored in Project Mariana (BIS Innovation Hub et al. 2023). These advantages diminish when activity is concentrated on a single governed platform or assets remain dispersed across different chains.

What a private platform provides

Under Project Helvetia, conducted with SIX since 2020, the SNB issues wCBDC on the SIX Digital Assets Platform, a regulated financial market infrastructure (FMI) that enables atomic settlement of cash and tokenized securities. Approximately USD 4 billion in digital bonds have been issued on the platform, with around half settled in wCBDC. On this permissioned platform, the central bank controls issuance and monetary functions, while an identifiable, supervised operator is responsible for operating the platform.

This model provides strong operational assurances, but its developer and application ecosystem is relatively small. Assets on other networks cannot interact natively with wCBDC, and the central bank depends on one platform operator. A public chain could offer access to a wider ecosystem of developers, assets, and applications, and allow native interaction with activities already on that chain. However, it would replace dependence on an identifiable operator with dependence on network participants who are not collectively bound by contractual service obligations. What safeguards could address that difference?

Three levels of control

On a permissionless blockchain, the protocol gives a central bank no special status. Monetary powers can be written into the token contract, but their timely exercise depends on the network. Table 1 distinguishes three levels of control and the off-chain arrangements that support them.

Asset level: authority over the monetary instrument

A token contract can reserve to the central bank powers to issue and redeem tokens, restrict direct holdings to eligible institutions, freeze addresses, pause transfers, execute forced transfers or redemptions, and upgrade the contract. To exercise these powers, the central bank must control the contract's administrative and upgrade keys. Issuance and redemption can be anchored to an RTGS account through a gateway that mints tokens only after the corresponding RTGS payment is final and releases funds only after the on-chain transfer is final. In the absence of a platform operator, this gateway becomes critical infrastructure in its own right.

Authority to act, however, is not the same as the ability to act in time. A freeze or pause is itself a transaction that the network must include. If the transaction is submitted publicly, the affected holder may see it and move funds before it takes effect. Congestion can also raise fees and delay inclusion during stress, precisely when time-critical central bank action may be needed.

Table 1. Levels of control over wCBDC on a public blockchain

Level	What it covers	Central bank control	Main residual dependency
Asset	Token contract: issuance, redemption, eligibility, freezing, pausing, upgrades	Exclusive authority over token functions, subject to control of administrative and upgrade keys	Timely network execution of those functions
Application	Contracts that hold or transfer wCBDC: settlement, escrow, collateral, trading	Decides which contracts to admit, but cannot unilaterally change their code	Upgrade authority of admitted contracts, greater exit complexity as composability deepens
Network	Transaction inclusion and ordering, finality, fees, data visibility, protocol upgrades	None directly; can select the network, define legal rules and prepare an exit plan	Validators and block builders, congestion, protocol changes, forks, and fees
Off-chain foundation	Rulebook, legal finality, participation agreements, RTGS gateway, monitoring	Authority over the rulebook, within the applicable legal framework	Legal recognition of finality linked to network events

Application level: a trade-off

Much of a public chain's value comes from interaction with third-party contracts, including exchanges, escrow, collateral applications and lending protocols. The token contract can check the immediate parties to a transfer, but it may not identify the beneficial users of a pool. The central bank must therefore decide which contracts to admit, considering their code, upgrade rights, beneficial-ownership arrangements and capacity to support orderly redemption. Admission conditions can limit the risks. Contracts might, for example, be required to remain immutable, subject upgrades to a timelock or a central bank veto, or use token standards that extend eligibility checks to indirect holders. Each additional application can expand exposability, but it may also weaken effective eligibility control and make exit harder, as discussed below.

Network level: outside central bank control

Validators and block builders, who may be located anywhere and need not meet the central bank's eligibility requirements, influence which transactions are included and in what order. No single counterparty can commit to network-wide service levels, incident response or protocol upgrades. Protocol changes emerge through an open community process, and disputed changes can split the network, as in the 2016 separation of Ethereum and Ethereum Classic. Restricting who may hold wCBDC does not restrict who may order its transactions. Front-running and strategic reordering therefore remain possible. The risk is limited for simple bilateral transfers between allowlisted institutions, but it becomes more important when wCBDC is used in automated market makers or lending pools. Exposure to transaction reordering thus grows with the range of admitted applications.

Network fees create another dependency. On Ethereum, transactions require gas fees denominated in ETH, exposing participants to the availability and price of a volatile native asset. Relayers or fee-payment services can spare individual institutions from holding ETH directly, but introduce further operational and governance dependencies. Protocol changes can also affect the assumptions underlying application controls. Ethereum's EIP-7702, introduced in 2025, allows externally owned accounts to delegate execution to smart-contract code. An approved account can therefore acquire functionality that was not envisaged when it was admitted, even though the holder allowlist remains intact. Conversely, a central bank may be unable to secure a protocol change that it considers necessary.

Confidentiality poses a further challenge. A public ledger exposes balances and transaction flows. Because wholesale participants are relatively few and often identifiable, pseudonymous addresses provide limited protection. Public visibility of banks' wCBDC balances or use of central bank credit could create stigma and financial-stability risks. Issuing wCBDC with publicly visible balances and transactions would therefore be difficult to reconcile with wholesale confidentiality requirements. Privacy technologies, including zero-knowledge proofs, computation on encrypted data and secure hardware, could help. But they increase complexity, may limit interaction with other applications and, depending on the design, can create dependencies on trusted service providers or governed components. Privacy-preserving implementations need not, however, move execution off Layer 1.

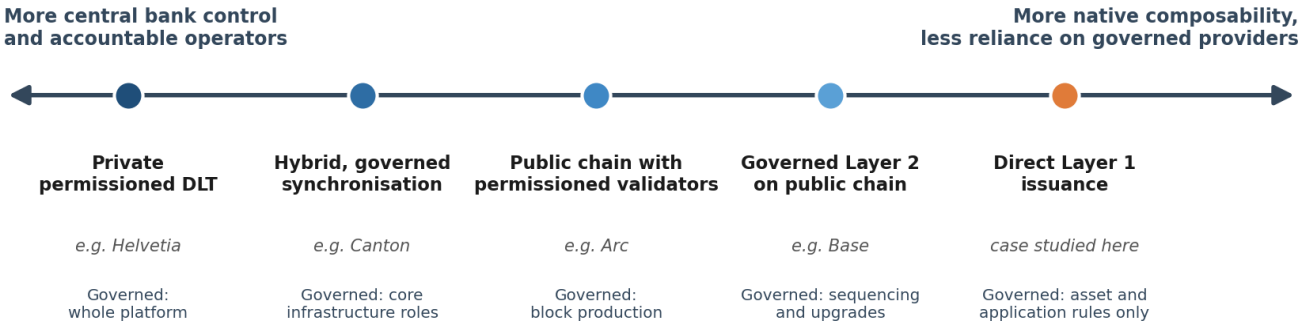
Possible measures to recover network-level assurances include private transaction-submission channels, arrangements for more predictable inclusion, resilient connectivity, a Layer 2 with transaction ordering performed by an accountable operator, or a permissioned validator set. Several of these measures introduce reliance on service providers. These choices form the spectrum discussed next.

A spectrum, not a binary choice

Design choices vary in the central bank's authority, native composability with the public ecosystem, and reliance on governed infrastructure providers. Greater control generally requires limiting permissionless interaction, relying on identifiable intermediaries or operating some infrastructure directly. Permissioning can apply separately to token holdings, applications, transaction ordering, and consensus. No architecture maximizes all objectives. Figure 1 illustrates representative choices.

Figure 1. The permissioning spectrum

Illustrative positions; each design places governed components at a different level



Market practice already spans several points on this spectrum. JPMorgan's deposit token JPMD became available to institutional clients on Base, an Ethereum Layer 2, in November 2025 and was extended to Ethereum Layer 1 in October 2026. Tokenized funds such as BlackRock's BUIDL operate on public chains but restrict transfers to approved investors. Circle's Arc launched its public mainnet in September 2026 with a permissioned set of institutional validators. At the same time, private platforms are adopting common standards and connecting to external chains.

For central banks, the policy question is which functions must be governed, at what level, and which residual dependencies are acceptable.

Regulation, finality and liquidity

Regulatory perimeter. The PFMI and national settlement-finality frameworks, including the EU Settlement Finality Directive (SFD) and the Swiss Financial Market Infrastructure Act (FinMIA), generally presuppose identifiable systems,

participants and rules. A permissionless blockchain has no operator responsible for the network as a whole. Instead, the relevant unit of assessment could be the wCBDC arrangement: its rulebook, token contracts, eligibility framework, RTGS gateway, monitoring and contingency functions. An identifiable entity would be responsible for the arrangement, which could be assessed against the relevant PFMI principles without prejudging its legal classification under national law. CPMI-IOSCO (2022) adopted a comparable functional approach to stablecoin arrangements. In Switzerland, FINMA licensed BX Digital, now SeturionX, as a DLT trading facility even though it settles securities on public Ethereum (FINMA 2025). The regulated FMI is the facility, not Ethereum. The underlying network is therefore an external operational dependency that must be managed through technical assessment, monitoring, contingency planning and exit arrangements.

Finality. Technical finality, the point at which a transaction is sufficiently unlikely to be reversed under a protocol's rules, differs from legal finality, the point at which it becomes irrevocable under applicable law. Both differ from settlement assurance: whether a transaction can be included and finalized within a predictable period. An arrangement's rulebook could define when a payment enters the system and when it becomes irrevocable, by reference to specified network events. But contractual rules alone cannot confer statutory finality protection. Whether such protection applies when state transitions are produced by validators outside the arrangement's control remains an open legal question, particularly in the event of a contested fork.

Liquidity. wCBDC would create another place in which participants hold central bank money. They might need to divide liquidity between RTGS accounts and the chain. Fragmentation across imperfectly connected systems can increase required balances and funding costs (Duffie 2026). A blockchain that operates continuously does not, by itself, ensure continuous access to additional central bank liquidity: that depends on RTGS operating hours and the central bank's credit and collateral arrangements. Intraday credit might be provided by minting tokens against collateral, but those transactions would still compete for blockspace under stress. On a transparent ledger, recourse to central bank credit could also become visible at the level of individual institutions. Overnight and emergency lending would therefore require arrangements that preserve confidentiality, potentially keeping these operations off-chain.

Exit and recovery as essential safeguards

Dependencies on the network cannot be eliminated through asset- or application-level controls alone. Credible recovery and exit arrangements are therefore essential. Exit should be the last step in a graduated response, from suspending issuance through restricting transfers and requiring redemption to winding down. Potential triggers include a contested fork, a prolonged failure to finalize transactions, excessive concentration among validators or block builders, sustained censorship of wCBDC transactions, an unpatchable vulnerability, adverse legal changes or the declining relevance of the chain. An orderly transition could involve migration to a new contract on the same chain, reissuance of recognized holdings on another platform, redemption into RTGS balances or settlement of tokenized assets through an RTGS link.

A key insight is that exit becomes more difficult as composability deepens. Direct holdings by identified institutions can usually be attributed and redeemed relatively easily. Positions in liquidity pools, lending protocols or collateral arrangements, however, may require valuation and termination under terms the central bank did not set. The integration that creates the benefits of a public chain can therefore also increase the cost of leaving it. One response is to make orderly exit a condition of admission: a contract could hold wCBDC only if it can attribute claims to beneficial owners and support redemption or migration under predefined rules.

Four safeguards are therefore essential for deploying wCBDC on a public chain. First, the central bank needs independent records sufficient to reconstruct every recognized claim at a legally specified point in time. Second, control functions must be tested under congestion, with procedures for determining and settling claims off-chain if the chain halts or censors transactions. Third, the rulebook must establish in advance the legal basis for suspending transfers and extinguishing on-chain claims when settlement takes place through RTGS. Fourth, exit procedures must be rehearsed periodically.

Conclusion

Direct issuance of wCBDC on a public blockchain is technically feasible in principle. The harder question is institutional. Central banks already depend on infrastructure they do not operate, but they typically manage those dependencies through contracts, oversight, and redundancy. The distinguishing feature of a public permissionless blockchain is the absence of an operator or contractual counterparty responsible for the underlying network. The wCBDC arrangement must therefore provide its own gateway, monitoring, legal finality rules, liquidity arrangements and recovery procedures.

Important questions remain. Can a legally defined settlement arrangement obtain statutory finality protection when its rules rely on state transitions outside the operator's control? Can time-critical central bank actions receive quantifiable inclusion guarantees without permissioning transaction ordering? Which privacy techniques best protect wholesale confidentiality? How do exit costs increase with integration into third-party contracts, and can admission rules ensure that positions remain redeemable? Which protocol changes should trigger intervention or exit when the central bank lacks governance rights? The answers will determine whether technical feasibility can become an institutionally acceptable arrangement. These questions are also relevant to the Eurosystem's Appia initiative, which is assessing different DLT infrastructure models and aims to deliver a blueprint by 2028.

References

Adrian, T., et al. (2025), "Understanding Stablecoins", IMF Departmental Paper No. 2025/009.

Bindseil, U. and B. Duve (2026), "Tokenizing Central Bank Money on Public Blockchains", SUERF Policy Brief No. 1572.

BIS (2025), "The Next-Generation Monetary and Financial System", Annual Economic Report 2025, Chapter III.

BIS Innovation Hub, Banque de France, Monetary Authority of Singapore and Swiss National Bank (2023), Project

Mariana: Cross-Border Exchange of Wholesale CBDCs Using Automated Market-Makers, Final Report.

CPMI-IOSCO (2012), Principles for Financial Market Infrastructures.

CPMI-IOSCO (2022), Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements.

Du, C., R. Sonawane and C. Watsky (2025), "In the Shadow of Bank Runs: Lessons from the Silicon Valley Bank Failure and Its Impact on Stablecoins", FEDS Notes, 17 December.

Duffie, D. (2026), "Tokenized Finance and the Perimeter of Central Banking", Jackson Hole Economic Policy Symposium, August.

ECB (2026a), "Pontes", ECB website.

ECB (2026b), "Appia – Paving the Way for a Future-Ready, Integrated Financial Ecosystem Leveraging Tokenisation and DLT", 11 March.

FINMA (2025), "FINMA Licenses First DLT Trading Facility", press release, 18 March.

Kosse, A., M. Glowka, I. Mattei and T. Rice (2023), "Will the Real Stablecoin Please Stand Up?", BIS Papers No. 141.

Schär, F., A. Kosse, T. Rice, T. Shirakami and J. Siridhasanakul (2026), "The Anatomy of Stablecoin Transactions", BIS Working Papers No. 1359.

About the author(s)

Jan Camenisch is a researcher at Category Labs. He also serves on Sovrin's Technical Governance Board. Before joining Category Labs, he was CTO at the DFINITY Foundation, and a Principal Research Staff Member at IBM Research, Zurich, where he was leading the Privacy & Cryptography research team and was a member of the IBM Academy of Technology. Jan Camenisch holds a PhD in Computer Science from ETH Zurich.

Julien Donnet is a Lead Product Manager at Taurus, where he works on blockchain infrastructure for institutional digital asset custody, tokenization, and trading. Before joining Taurus, he was Head of Product Management at SIX Digital Exchange (SDX). Earlier, he built blockchain and digital asset products at Citi Ventures. Julien Donnet holds an Executive MBA from EPFL and a master's degree from TELECOM Nancy.

Simon Lavater is a business development manager at SIX Digital Assets, specializing in digital securities, digital money, and DLT-based financial market infrastructure. His work spans tokenization, stablecoins, digital custody, and bridging traditional capital markets with emerging digital ecosystems. He holds a master's degree in business innovation from the University of St. Gallen.

Thomas Moser is an Alternate Member of the Governing Board of the Swiss National Bank, and a Visiting Professor at the University of Lucerne, Switzerland. Before joining the Swiss National Bank, he was an Executive Director at the International Monetary Fund (IMF) in Washington D.C., United States. Thomas Moser holds a PhD in Economics from the University of Zurich.

SUERF Policy Notes and Briefs disseminate SUERF Members' economic research, policy-oriented analyses, and views. They analyze relevant developments, address challenges and propose solutions to current monetary, financial and macroeconomic themes. The style is analytical yet non-technical, facilitating interaction and the exchange of ideas between researchers, policy makers and financial practitioners.

SUERF Policy Notes and Briefs are accessible to the public free of charge at https://www.suerf.org/publications/suerf-policy-notes-and-briefs/

The views expressed are those of the authors and not necessarily those of the institutions the authors are affiliated with.

© SUERF – The European Money and Finance Forum. Reproduction or translation for educational and non-commercial purposes is permitted provided that the source is acknowledged.

Editorial Board: Ernest Gnan, Jakob de Haan, David T. Llewellyn, Donato Masciandaro

Designed by the Information Management and Services Division of the Oesterreichische Nationalbank (OeNB)

SUERF Secretariat
c/o OeNB, Otto-Wagner-Platz 3A-1090 Vienna, Austria
Phone: +43 1 40 420 7206 E-mail: suerf@oenb.at Website: https://www.suerf.org/

ISSN 2791-5395 (Online)