SUERF
The European Money and Finance Forum

SUERF Policy Note
No 420, September 2026

Privacy in wholesale cross-border payments: Assessing Project Agorá

Jan Camenisch | Category Labs
Thomas Moser | Swiss National Bank

Keywords: Wholesale cross-border payments, Distributed Ledger Technology (DLT), privacy, Central Bank Digital Currency (CBDC), tokenized deposits

JEL codes: E42, E58, F33, G21, G28, O33, D82

Abstract

Privacy is a central challenge for distributed ledger technology (DLT). This note proposes five objectives that a privacy architecture for wholesale cross-border payments should meet and assesses the design of Project Agorá against them. Agorá provides strong confidentiality against non-involved participants, selective disclosure, multi-jurisdictional configurability and comparatively low privacy overhead. The design's principal trade-offs are reliance on issuer verification, metadata leakage, and the resilience requirements created by keeping private state off-ledger.

Disclaimer: The views expressed are those of the authors and do not necessarily reflect those of the SNB or of Category Labs. The authors would like to thank Remo Nyffenegger and The Project Agorá Team for comments.

Introduction

The Bank for International Settlements (BIS) and the Institute of International Finance (IIF) published on 27 May 2026 the prototype report for Project Agorá, a public-private initiative involving seven central banks and more than forty regulated financial institutions (BIS 2026).[1] The project seeks to improve correspondent banking by placing tokenized central bank reserves and commercial bank deposits on a shared, permissioned DLT platform. Its two-layer architecture comprises jurisdictional ledgers for each country or currency, which hold tokenized central bank reserves under the authority of the relevant central bank, and a unifying ledger on which tokenized commercial bank deposits are held and cross-border workflows are orchestrated.

Wholesale payment flows can reveal commercially sensitive information, e.g., about an institution's own business, underlying clients, or liquidity positions. These risks are amplified on DLT platforms shared by competing institutions. The challenge is to preserve transaction confidentiality while allowing validation, audit and disclosure to parties with legitimate operational, regulatory or supervisory needs.

This note assesses Project Agorá's privacy architecture. It first defines the objectives of a privacy architecture for wholesale cross-border payments, then surveys the main privacy-preserving techniques and finally examines how Project Agorá combines them.

Privacy Design Objectives

A privacy-respecting architecture for wholesale cross-border payments should meet the following five objectives:

1. **Confidentiality and selective disclosure**. Participants should see only the transaction information required for their role. Non-involved participants should not see amounts, counterparties or client information, while counterparties, operators and issuers should receive only what they need to perform their functions.

2. **Metadata and inference confidentiality**. Confidentiality should extend beyond transaction contents to information that can be inferred from transaction patterns, including aggregate positions, settlement behavior, transaction graphs, timing, and frequency.

3. **Verifiability without undue concentration of trust**. Concealment must not prevent parties or validators from verifying a transaction's validity, and confidentiality and verification should not require unnecessary concentration of information or control in a single party.

4. **Regulatory access and jurisdictional configurability**. AML/CFT, sanctions screening, audit and supervisory access must remain effective without unnecessary disclosure. Disclosure and policy rules must be adaptable across jurisdictions.

5. **Operational viability and composability**. The design must be scalable, resilient, durable and composable with the applications the platform is intended to support. Off-ledger state must remain available and recoverable, cryptographic components replaceable as assumptions and standards evolve, and confidentiality mechanisms should not unduly constrain applications involving multiple participants or shared state.

These objectives involve unavoidable trade-offs. Stronger concealment may reduce independent verifiability or supervisory visibility, and distributing data can complicate audit and recovery. A workable architecture must balance these competing objectives deliberately.

[1] The central banks are Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England, and the Federal Reserve Bank of New York. The Bank of Canada subsequently joined the project, bringing the number of participating central banks to eight.

Relevant Privacy-Preserving Techniques

Two broad approaches are relevant. (i) Generic secure-computation technologies evaluate programmable functions over private inputs. They can often accommodate changed requirements by changing the program being computed, and a mature platform can spread the cost of security testing across applications. Their main drawback is computational or communication overhead. (ii) Tailored protocols instead combine purpose-built cryptographic primitives for greater efficiency, but require application-specific security analysis and are generally harder to modify. A special-purpose protocol can provide strong assurance for its intended use; the difference is one of adaptability and cost of assurance, not an inherent security ranking. Practical systems may combine both approaches.

Secure multi-party computation (MPC) lets several parties compute jointly over private inputs, revealing only the result. It normally relies on secret sharing or garbled circuits and avoids a single trusted party as long as fewer than a specified threshold collude. Its principal cost is interactive communication. Fully homomorphic encryption (FHE) permits computation directly on ciphertexts. A computing party can produce an encrypted result without learning the inputs, and threshold decryption releases only the intended result.. Trusted execution environments (TEEs) instead process plaintext inside attested hardware enclaves. They offer near-native performance but shift trust to the hardware manufacturer, the attestation mechanism and the enclave's resistance to side-channel attacks.

Tailored payment protocols commonly combine commitments, encryption, signatures, and zero-knowledge proofs. A commitment conceals a value while binding the committer to it. A zero-knowledge proof can establish, for example, that a transaction is well formed, that the sender owns the inputs, and that value is conserved without revealing amounts or balances. Succinct systems such as zk-SNARKs and zk-STARKs can make verification inexpensive even when proof generation is demanding.

Zero-knowledge proofs are a proving technique rather than a complete privacy architecture. The private state must still be committed to or encrypted, distributed to the appropriate parties and kept available. Standard proofs also require the prover to know the private inputs, which can be restrictive when data are held across several parties; those cases may require MPC or another distributed-computation technique. Also, systems marketed as "zero-knowledge," notably many zk-rollups, often use proofs only to ensure correctness while leaving transaction data public. Verifiable computation is not necessarily confidentiality.

The practical design space has widened as proof systems have become more efficient. Earlier systems worked best with specially chosen, proof-friendly primitives (Camenisch and Lysyanskaya 2001). Common signatures, hashes and certificate chains were expensive to prove over. More recent techniques can support statements about standard credentials and policy checks (Frigo and shelat (2026), such as proving that an institution possesses a valid certificate or has completed KYC, without requiring the certificate or underlying customer data to be disclosed. These advances make zero-knowledge selective disclosure more relevant to regulated payment systems, although system integration and proving costs remain material.

These mechanisms protect transaction contents, not communication and workflow metadata. Padding, batching and cover traffic can obscure message size and timing; mix networks and onion routing can obscure communication relationships; and path-aware architectures such as SCION can limit which networks observe a communication path (Cimaszewski et al. 2025). The techniques impose different costs in bandwidth, latency, and infrastructure.

Strong theoretical guarantees also do not prevent leakage through implementation flaws, side channels, protocol composition or user behavior. Statistical analysis has, for example, weakened the practical anonymity of some ring-signature systems by exploiting transaction-selection patterns (Möser et al. 2018), while TEEs have been vulnerable to hardware side channels. These examples show that effective privacy depends on implementation quality, key management, and operational procedures as well as cryptographic design.

Privacy Mechanisms Offered by Paladin

Project Agorá uses Paladin, an open-source privacy framework for ledgers running the Ethereum Virtual Machine (EVM), which is a widely used smart-contract execution environment. Paladin is developed under LF Decentralized Trust (LF Decentralized Trust 2026). It packages privacy mechanisms as pluggable "domains," allowing different confidentiality models to operate on the same base ledger and additional domains to be added through a common interface. Its built-in domains include Pente, Noto and Zeto. We discuss all three, although the prototype uses only Pente and Noto. Zeto provides a useful zero-knowledge benchmark.

Pente provides private smart-contract execution for a defined "privacy group." For each transaction, it loads the required state into an ephemeral in-memory EVM, executes the contract and records masked commitments to the inputs and outputs on the shared ledger. Group members endorse the transition and retain the underlying data; outsiders see only opaque commitments. Group membership is fixed when the group is created, but its members can deploy multiple contracts within the private environment.

Noto is a confidential token model of the unspent-transaction-output (UTXO) type, in which value is held as discrete coins that are consumed and recreated by each transfer rather than as account balances. A coin contains an owner, amount and random salt (i.e., a random value mixed into the hashed data so that the resulting hash cannot be reversed by testing likely amounts or owners), but only its hash is recorded on the base ledger; the underlying data are exchanged privately among entitled parties. Each transfer is endorsed by a notary, normally the token issuer. The notary sees the full transaction and validates request authenticity, ownership, value conservation and applicable policy conditions, while the base ledger provides final double-spend protection. Other participants see only their own holdings. Noto's approval logic can itself be implemented in Pente, and coins can be locked subject to release conditions to support atomic delivery-versus-payment.

Zeto represents value through similar commitments but replaces notary verification with zero-knowledge proofs. The chain can verify ownership, non-double-spending and value conservation without learning amounts or counterparties. Different circuits can add encrypted transfers, KYC-bound ownership or stronger anonymity, at increasing computational cost. Compared with Noto, Zeto reduces issuer visibility and strengthens independent verifiability but requires proof-generation infrastructure. Agorá's choice of Noto reflects its institutional setting: the issuers are identified regulated entities.

Assessing Project Agorá Against the Five Objectives

Confidentiality and selective disclosure (Objective 1)

Agorá combines Noto commitments with Pente privacy groups. Non-involved participants see neither payment contents nor the private workflow, although shared-ledger workflow events and commitments remain observable. Counterparties and issuers receive the information required for their roles. Compliance results can be shared as coded attestations rather than underlying customer data. This is a strong fit for a permissioned wholesale setting, which requires confidentiality from other participants but not payer anonymity from the issuer.

Client-data protection depends on architecture as well as cryptography. The platform serves institutions and corporates rather than consumers, so personal-data rules may often concern only incidental information; customer-confidentiality and bank-secrecy obligations nevertheless remain relevant. Features such as confirmation of payee and compliance flags may require consent or carefully limited disclosure. The need-to-know allocation of data is therefore a substantive part of the privacy design.

The architecture also reduces the conflict between DLT immutability and rights to erasure. Only salted commitments are written on-chain; payloads and opening information remain off-ledger. Deleting all information that can link a commitment to a person or transaction may render the commitment effectively unlinkable, although whether this constitutes erasure depends on applicable law and the completeness of deletion (EDPB 2026a, 2026b). A corrected

state can supersede an earlier state, but does not alter the historical ledger. The same private data must therefore be recoverable after failures yet reliably deletable when required.

Alternative systems conceal transactions through different trust models. In Zcash-style systems, anyone can verify a zero-knowledge proof without seeing the transaction data; in Noto, assurance rests on the notary's access to the full state. Zcash viewing keys can support selective disclosure, but disclosure is generally controlled by the holder. For an identified, permissioned membership, Agorá's commitment-plus-privacy-group approach avoids anonymity properties the wholesale setting does not seek, but it also forgoes independent verification of concealed transfers.

Metadata and inference confidentiality (Objective 2)

Agorá conceals individual amounts and balances, but validators, node operators and privacy-group members may still observe the timing and number of anchors (i.e., records on the shared ledger), workflow stages, endorsement requests, group participation, exceptions and delays. These patterns may reveal correspondent relationships, settlement behavior or liquidity stress. A cluster of exceptions, timeouts and late-session endorsements around a quarter-end reporting date could, for example, provide a plausible signal of funding stress. Permissioning narrows the set of observers but does not remove the risk, since participants include competitors.

Payload encryption alone cannot address these inferences. Application-layer measures may batch or randomize settlement and anchoring, reduce distinguishable workflow events or conceal group membership. Network-layer measures may pad messages, add cover traffic, segment communication or control routing paths. The appropriate combination depends on the sensitivity of the metadata and the performance cost that the system can bear.

Verifiability without undue concentration of trust (Objective 3)

Agorá preserves correctness through delegated rather than trustless verification. Noto's salted hashes do not allow validators to verify value conservation independently; the issuer-notary sees the full token state and attests to validity. Correctness is preserved, but the issuer becomes a concentration point for information and trust as well as availability.

This trade-off differs by asset. For central-bank reserves, the central bank is a non-competing public authority and already observes transfers in its real-time gross settlement system (RTGS). Notary visibility therefore introduces nothing new. For commercial-bank deposit tokens, however, the issuer is a market participant and may see transfers between third parties, including competitors. This resembles the visibility of an account-servicing institution, but in Noto it follows from the verification design rather than from executing the payment. This is a genuinely novel exposure, particularly where a deposit token circulates beyond the issuer's own customer base, where the issuer is not otherwise on the payment path, or in the aggregate view the notary acquires across the shared unifying ledger. The safeguard against misuse is consequently organizational rather than cryptographic. A Zeto-like model could reduce this visibility, at the cost of heavier proof generation and more complex regulatory access.

At the workflow level, Pente provides a more distributed form of assurance. Anchoring output-state commitments on the base ledger makes inconsistent views among privacy-group members detectable rather than silent. It does not make the private computation publicly verifiable, but strengthens consistency among the parties that rely on it.

Regulatory access and jurisdictional configurability (Objective 4)

Agorá is designed for selective disclosure rather than anonymity. Institutions perform AML/CFT, sanctions, KYC and fraud checks in their own systems, while issuers, auditors and other authorized parties can substantiate token-state transitions from the off-chain data they hold. The controls required for wholesale payments therefore remain operable. Supervisory and audit access is reconstruction from institutional records rather than a platform capability, and therefore relies on governance arrangements for access that the prototype left out of scope.

Disclosure of an outcome does not end the privacy analysis. A binary pass/fail flag may itself reveal sensitive information, e.g., by creating tipping-off concerns if a failure suggests that a suspicious-activity report is being

considered. Zero-knowledge predicates or an MPC-based calculation could reduce this leakage, although at additional cost and complexity.

Other permissioned platforms, including Fabric, Quorum, Corda, and Canton, follow a similar need-to-know principle by restricting transaction visibility to relevant parties. A more cryptographically ambitious model would use zero-knowledge selective disclosure, e.g., a proof that screening was completed, without revealing either the underlying data or a detailed compliance outcome. Agorá's coded attestations are operationally simpler, but their information content should be assessed explicitly.

The two-layer architecture is well suited to jurisdiction-specific requirements. Each central bank controls the rules for its jurisdictional ledger and tokenized reserves, while the unifying ledger coordinates cross-border settlement. Disclosure and policy rules can therefore vary by jurisdiction and currency without fragmenting the platform. This architectural configurability is one of the prototype's clearest strengths.

Operational viability and composability (Objective 5)

Agorá keeps computational and cryptographic privacy overhead low by processing private information in participant off-ledger middleware and privacy groups, and anchoring only commitments on-ledger. It avoids per-transaction zero-knowledge proofs, MPC communication rounds and FHE's computational burden.[2] Its mechanisms also compose naturally for bilateral applications: locked coins and private workflows can support atomic delivery-versus-payment across tokens. Composability with applications that rely on shared mutable state is less straightforward. The principal unresolved issues therefore include the availability and recovery of private off-ledger state, the liveness of notaries, and composability with shared-state applications.

Production use must also demonstrate scalable privacy-group management: the number of groups, their membership, private-state growth, and coordination overhead will increase as more institutions, jurisdictions and currencies are added. The prototype must also show that regulatory and audit access works reliably in practice and that cryptographic components can be replaced as security assumptions and standards evolve.

Table 1. Assessing Project Agorá against the five privacy objectives

PRIVACY OBJECTIVE	AGORÁ: MAIN STRENGTH	MAIN TRADE-OFF / RESIDUAL ISSUE
1. Confidentiality and selective disclosure	Transaction contents are concealed; non-involved participants see only commitments, spend references and public ledger metadata. Relevant parties receive private data on a need-to-know basis.	Confidentiality depends on correct allocation and protection of off-ledger private state, which must be securely retained, recovered and, where required, deleted.
2. Metadata and inference confidentiality	Individual amounts, balances and private transaction contents are concealed from non-involved participants.	Anchors, workflow events, timing, participation, exceptions and communication patterns can reveal relationships, settlement behaviour or liquidity stress.
3. Verifiability without undue concentration of trust	Double-spend prevention is chain-enforced; Pente anchors make inconsistent views among privacy-group members detectable.	Verification relies on issuer/notary visibility and availability, concentrating information and operational dependence.
4. Regulatory access and jurisdictional configurability	AML/CFT, sanctions, audit and supervisory access are preserved; two-layer design lets jurisdictional disclosure and policy rules differ.	Compliance outcomes can reveal sensitive information. Supervisory access is not a platform capability but by reconstruction from off-chain records. Governance of such data is left out of scope.
5. Operational viability and composability	Privacy overhead is structurally low: the design avoids per-transaction proofs, MPC communication rounds and FHE evaluation.	Key open issues are off-ledger state recovery, key management, notary liveness, privacy-group scaling, shared-state composability and cryptographic agility.

[2] This is an architectural claim. The prototype did not benchmark privacy overhead, and throughput, latency, operational resilience and failover were outside the scope of the phase reported.

Areas for Further Work

Real-value testing in a controlled environment took place in July 2026, involving twenty-eight financial institutions and central banks and a limited set of currencies and scenarios. It was not designed to test the privacy properties discussed here, so the following remain open.

Off-chain private state. The data and keys retained by participants are necessary to interpret commitments, complete workflows, support audit and resolve disputes. Future phases should test key generation, custody, rotation, recovery, and revocation; reconstruction after outages, cyber incidents or participant failure; and continuity when institutions join, leave or disconnect. Losing the data needed to reconstruct private state could impair settlement, auditability, and business continuity even though the shared ledger remains intact. State-management rules must reconcile resilience with legally required deletion.

Metadata leakage. Testing should establish what different observers can infer at the ledger, workflow and network layers. It should cover commitments, privacy-group contracts, anchors, timeouts, endorsement requests, message headers, routes, sizes and timing. A measured baseline is needed before mitigations can be compared. Batching, randomized timing, padding, cover traffic, network segmentation, concealment of group membership and path-aware routing should then be evaluated for both privacy gain and operational cost.

Production-scale operation and access. Exercises involving sanctions investigations, AML/CFT procedures, supervisory requests, audits, and disputes should verify that authorized access works promptly and reliably without exposing unrelated transactions. They should also cover notary and endorsement availability, including failover when an issuer or group member is unreachable.

Composability with shared-state applications. Agorá's privacy mechanisms compose naturally for bilateral applications such as atomic delivery-versus-payment, but shared mutable state poses a harder problem. Privacy-preserving computationapproaches such as MPC or trusted execution may mitigate this trade-off. Future phases should therefore assess how confidentiality interacts with composability.

Cryptographic durability. Salted hashes plausibly provide quantum-resistant hiding, but authentication, endorsement signatures, certificates and encrypted channels rely on public-key cryptography. Future phases should plan migration to post-quantum signatures and key exchange, taking account of the required lifetime of confidential data.

Conclusion

Agorá has an operationally pragmatic privacy design. It provides strong confidentiality against non-involved participants, selective disclosure, regulatory access and multi-jurisdictional configurability at comparatively low computational cost. These benefits are obtained by relying on issuer verification and by holding private state off-ledger. The prototype demonstrates that token confidentiality and private workflow execution can be combined on a shared DLT platform. Its practical viability will depend chiefly on robust management of off-chain state and on reducing leakage from workflow and network metadata. One option worth examining is whether data availability layers could ensure retrievability of encrypted private state. A broader question is how far Agorá's design principles could be realized on a public permissionless blockchain.

References

BIS Innovation Hub. 2026. Project Agorá: A shared programmable platform for wholesale cross-border payments, 27 May. https://www.bis.org/publ/othp110.htm.

Camenisch, Jan, and Anna Lysyanskaya. 2001. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation." In Advances in Cryptology — EUROCRYPT 2001, edited by Birgit Pfitzmann, 93–118. Lecture Notes in Computer Science 2045. Berlin: Springer.

Cimaszewski, Grace, Francesco Da Dalt, Thomas Moser, Adrian Perrig. 2025. "SCION and cross-border payments: Enhancing security and compliance in distributed ledger networks." SNB Working Paper 2025-15.

European Data Protection Board (EDPB). 2026a. Guidelines 02/2025 on Processing of Personal Data through Blockchain Technologies. Version 2.0, adopted 7 July 2026. https://www.edpb.europa.eu/documents/guideline/guidelines-on-processing-of-personal-data-through-blockchain-technologies_en.

European Data Protection Board (EDPB). 2026b. Guidelines 02/2026 on Anonymisation. Adopted 7 July 2026.

Frigo, Matteo, and abhi shelat. 2026. "Anonymous Credentials from ECDSA." IACR Communications in Cryptology 3 (1). https://doi.org/10.62056/a3qjmpgxq. Preprint at https://eprint.iacr.org/2024/2010.

LF Decentralized Trust. 2026. Paladin: Programmable Privacy for EVM. Documentation, https://lf-decentralized-trust-labs.github.io/paladin/

Möser, Malte, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. 2018. "An Empirical Analysis of Traceability in the Monero Blockchain." Proceedings on Privacy Enhancing Technologies 2018 (3): 143–163.

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.

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/.

Editorial Board: Ernest Gnan, 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)