Share intelligence. Not data.

More time for relevant investigations

Money-laundering networks move across institutions. Each bank sees a fragment, and investigators must decide which signals merit attention. The BIS's 2023 Project Aurora report cites an estimate that 90–95% of alerts from rules-based monitoring are false positives. Reviewing those alerts consumes investigation capacity. [1]

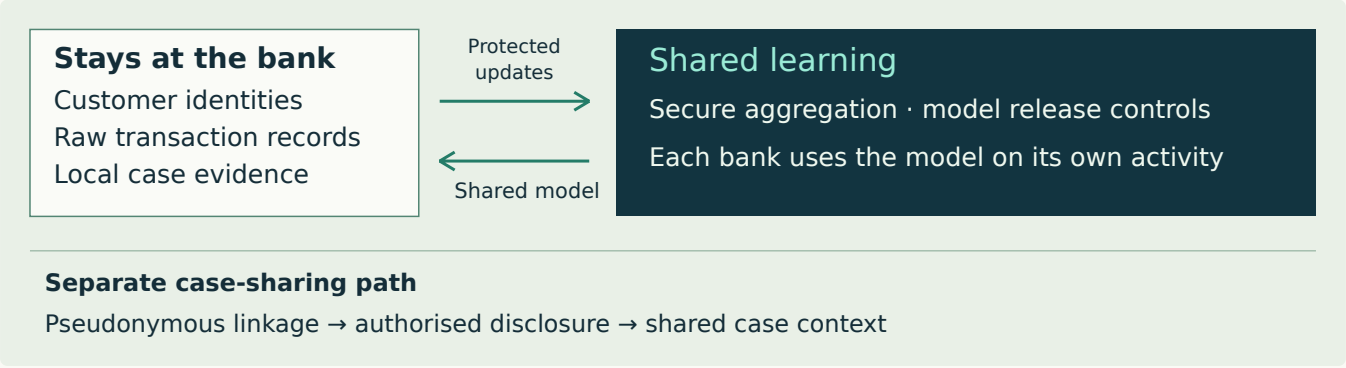
Node16.ai connects detection and investigation while each bank retains control of its raw records and customer identities.

Sonar: find the activity worth investigating

Sonar combines graph-based detection with bank-local pattern analysis. It scores transactions and relationships so investigators can assess relevant findings at their available capacity. Hybrid federated learning lets banks contribute to a shared model without pooling their raw transaction records. Models are trained and evaluated on synthetic data using sovereign supercomputing infrastructure.

Investigator: turn a signal into a reviewed case

Investigator includes Sonar and adds case intake, triage, graph exploration, evidence queries, KYC context and evidence-linked narrative and goAML reporting preparation. The investigator and MLRO retain decisions and reporting authority. A bank can start with its own case workflow; shared learning adds a further source of intelligence as participation grows.



Architecture illustration. Learning and case disclosure have distinct controls.

Development at scale

Approximately **4 billion synthetic transactions, 4 million customers and 187 money-laundering typologies** support development. Corpus coverage and a model's measured performance are distinct. Comparisons identify their model, baseline and operating point; synthetic evidence does not establish real-bank results.

Control through the whole workflow

Raw transaction records, customer identities and bank-local case evidence stay in the bank-scoped environment. Protected model contributions support shared learning. The architecture combines graph neural networks, secure aggregation and differential-privacy release controls. The privacy claim must match the actual mechanism, contribution unit and release sequence; synthetic testing is not proof of complete production subject-level privacy.

Banks derive pseudonymous linkage tokens from verified customer or entity identifiers using keyed cryptographic functions and common normalisation. This supports linkage without exchanging names or original identity numbers in that process. Link quality, key custody and access remain governed.

The secure-aggregation session design uses **ML-KEM-768**, standardised in NIST FIPS 203, for bank-to-bank key establishment. It is intended to resist attacks on recorded exchanges by future quantum computers. This concerns those sessions, not every API connection or authentication mechanism.

Collaborator: share more when there is authority to share

Collaborator is the planned information-sharing offering under AMLR Article 75, targeted for **July 2027**. It develops limited signals into shared case context as risk, purpose and authority justify disclosure. This is a separate path from shared model training, with recipient-specific access and recorded human decisions.

Oversight spans all three products: risk tolerance, roles, model versions, review and an attributable audit trail. Node16.ai coordinates the service; participant roles, model-change approval and supervisory visibility are part of the partnership arrangements. The ISO/IEC 27001 programme is in progress.

Why now, and how to begin

The AMLR's main application date is 10 July 2027. [2] Node16.ai is participating in a regulatory sandbox to clarify the relationship between AMLR, GDPR and the AI Act, aiming for commercial clarity in **Q1 2027** in Denmark and beyond. Low-touch, semi-guided and fully outsourced engagement options are being developed with banks and regulators; responsibilities follow the agreed engagement.

The company brings banking and compliance work together with legal experience and applied AI research. Henrik Axelsen is a former practising lawyer, former senior partner at two Big Four firms serving banks' risk and compliance functions and a serial founder. He holds a PhD in computer science and conducts research in AI and governance.

Request a product briefing: hello@node16.ai. Start with a synthetic walkthrough of Sonar and Investigator, then discuss your detection baseline, case workflow, integration and operating model.

[1] BIS Innovation Hub, Project Aurora, 31 May 2023, p. 19. Industry context, not a Node16.ai performance result. Source ↗

[2] Regulation (EU) 2024/1624, Article 90. Source ↗