SERIES	Boli Working Papers · Extract
AUDIENCE	Digitalisation
DATE	May 2026
ISSUED BY	Boli Association · Zurich
TECHNICAL	Tenzro Network · Tenzro Labs Pte. Ltd.

DIGITALISATION EXTRACT · MAY 2026

A digital archipelago and the substrate for sovereign automation.

National identity, verifiable credentials, sovereign and air-gapped compute, automated workflows under state mandate, and connectivity — where the Maldives' digital substrate sits relative to the standards consensus of 2026, a curated extract from the Boli Working Paper of May 2026.

SUBJECT

eFaas · Favara · TDIP · W3C Verifiable Credentials · eIDAS 2.0 · Agent Payments Protocol · Model Context Protocol · Trusted Execution Environment · sovereign AI · air-gapped AI · Tenzro Network · Canton sub-transaction privacy.

04°10′N 73°30′E

● Boli Association

ABOUT THIS EXTRACT

This document is a curated extract of the Boli Working Paper of May 2026, *The Maldives and the rewiring of global finance*. It selects the digital-identity, agentic-AI, sovereign-compute, privacy, and interoperability material from the full paper for a digitalisation-technology audience. The full paper is published separately and contains additional sections on institutional consolidation, sovereign asset surface, commercial banking adoption, and the Canton onboarding pathway.

EDITORIAL POSITION

The views expressed are those of the authors and do not necessarily reflect the views of the Boli Association, of its members, or of any external technical contributor including Tenzro Network and Tenzro Labs Pte. Ltd.

AVAILABILITY

This extract is available on the Boli Association website (boli.org).

A digital archipelago and the substrate for sovereign automation.

National identity, verifiable credentials, sovereign and air-gapped compute, automated workflows under state mandate, and connectivity — where the Maldives' digital substrate sits relative to the standards consensus of 2026, a curated extract from the Boli Working Paper of May 2026.

BOLI ASSOCIATION • TENZRO NETWORK • TENZRO LABS PTE. LTD.

ABSTRACT

The institutional consensus on artificial-intelligence integration in payments — articulated across the International Monetary Fund's *How Agentic AI Will Reshape Payments* note of April 2026, the Bank for International Settlements' 2025 *Annual Economic Report* Chapter III, and the supervisory work of the International Organization of Securities Commissions and the Financial Stability Board — places probabilistic AI in an upstream orchestration layer, deterministic rule-based controls in an authorisation layer beneath it, and irrevocable settlement in a separate finality layer beneath both. Model-risk and accountability obligations attach to the AI layer and do not migrate downward.

KEYWORDS

eFaas · OneGov · Favara · UPI · TDIP decentralised identifiers · W3C Verifiable Credentials Data Model 2.0 · SD-JWT VC · BBS+ · ISO 18013-5 mDoc · eIDAS 2.0 · Agent Payments Protocol · x402 · Model Context Protocol Identity · Trusted Execution Environment · Intel TDX · NVIDIA H100/H200 · AMD SEV-SNP · Tenzro Network decentralised compute · air-gapped AI · sovereign AI · Canton sub-transaction privacy · FROST · MPC wallets · post-quantum cryptography.

SUBJECT

digital identity · agentic AI integration · sovereign compute · data residency · verifiable credentials · cross-chain interoperability · SIDS digitalisation policy.

Executive summary

The institutional consensus on artificial-intelligence integration in payments — articulated across the International Monetary Fund's *How Agentic AI Will Reshape Payments* note of April 2026, the Bank for International Settlements' 2025 *Annual Economic Report* Chapter III, and the supervisory work of the International Organization of Securities Commissions and the Financial Stability Board — places probabilistic AI in an upstream orchestration layer, deterministic rule-based controls in an authorisation layer beneath it, and irrevocable settlement in a separate finality layer beneath both. Model-risk and accountability obligations attach to the AI layer and do not migrate downward.

The same supervisory bodies have named **THIRD-PARTY DEPENDENCY ON A SMALL NUMBER OF ARTIFICIAL-INTELLIGENCE SERVICE PROVIDERS** as a systemic concern. The decentralised-compute response — an open-source compute marketplace with **Trusted Execution Environment attestation** across an open provider population and **air-gapped artificial-intelligence model deployment** on the same protocol surface — closes the data-sovereignty objection that has slowed sovereign and bank-side AI adoption through 2024 and 2025.

For the Maldives — eighty per cent of its population over the age of ten enrolled in the eFaas national identity, the highest-enrolment national identity in the small island developing state group; a domestic instant-payments rail (Favara) integrating with India's Unified Payments Interface from July 2026; nationwide fibre-to-the-home completed in January 2025; four submarine cables landed and a fifth (the Google Dhivaru system) announced in November 2025; commercial 5G live since 2019; Starlink licensed since August 2023 — the question is how that digital substrate composes with the verifiable-identity, agentic-runtime, and sovereign-compute primitives the global standards bodies have crystallised in 2025–2026.

This extract presents the digitalisation, identity, AI-integration, sovereign-compute, privacy, and interoperability material from the full Boli Working Paper of May 2026, for a digitalisation-technology audience.

1. The Maldives' digitalisation and connectivity record

Across the thirty-nine United Nations-recognised small island developing states, the empirical record of blockchain and digital-currency initiatives between approximately 2018 and 2026 places the Maldives as the jurisdiction with the strongest documented digital-finance infrastructure in the group — measured by enrolment in identity, by adoption of instant payments, and by the alignment between the two.

The eFaas national identity platform, operated by the National Centre for Information Technology, enrols approximately two hundred and seventy-two thousand individuals, roughly eighty per cent of the population aged ten and above, as reported in late 2025. The OneGov platform at one.gov.mv aggregates services from multiple government agencies under eFaas.

A multifunctional Smart-ID card with integrated Mastercard payment rails is scheduled for rollout in 2026, anchored in a five-year Digital Country Partnership memorandum of understanding signed in October 2025 between Mastercard, the National Centre for Information Technology, and the Bank of Maldives.

The system is, in 2026, the highest-enrolment national identity in the small island developing state group and is paired institutionally with payment rails in a way that no other jurisdiction in the group has yet achieved. The platform uses facial-recognition biometrics and a centralised registry rather than a verifiable-credential wallet pattern.

Verifiable-credential conformance under the World Wide Web Consortium's Verifiable Credentials Data Model 2.0 (which became a W3C Recommendation on the fifteenth of May 2025) and formal mutual recognition under the European Union's eIDAS 2.0 framework are, accordingly, greenfield integration work rather than off-the-shelf capability.

The Favara instant-payments platform — built by the Nordic technology partner Tietoevry, launched by the Maldives Monetary Authority in late August 2023, and built to International Organization for Standardization 20022 messaging — handles a large share of domestic retail transaction volume on Maldives Monetary Authority reporting, with the Maldives Monetary Authority publishing monthly payments-bulletin disclosures of throughput. The Maldives Monetary Authority's agreement with India's

NPCI International (NIPL) integrates Favara with the Unified Payments Interface, with person-to-person cross-border functionality scheduled for July 2026 and merchant quick-response functionality following.

The digital-identity and instant-payments record sits inside a longer trajectory of state digitalisation and connectivity investment under both the Solih administration (November 2018 to November 2023) and the Muizzu administration (November 2023 to date), and that trajectory matters for the credibility of any tokenised-settlement layer built on top of it.

On the digital-government side, the Solih period saw the One-Gov services platform stood up, foundational work on the modern eFaas implementation, the Whistleblower Protection Act enacted, and the World Bank-financed Digital Maldives programme advanced through the Ministry of Environment, Climate Change and Technology and the National Centre for Information Technology. The Muizzu period has added the Maldives 2.0 / Digital 2.0 framework inaugurated at a Digital Transformation Summit in Malé on the ninth of May 2025, an Artificial Intelligence Masterplan 2025–2035 announced after a Cabinet meeting on the sixteenth of October 2024 with the National Centre for Information Technology as lead implementing agency, the Mastercard Digital Country Partnership signed in October 2025, the Bank of Maldives Swipe multicurrency wallet unveiled in October 2025 with a beta release in December 2025, and the Maldives International Financial Centre announcement of the fifth of May 2025 with its publicly stated blockchain and real-world-asset-tokenisation mandate.

The Ministry of Finance operates the Bandeyri budget-execution portal, the Beelan e-procurement system, and the Neelan inventory system as the public-finance digital backbone. In the 2024 United Nations E-Government Survey the Maldives ranked ninety-fourth globally at a score of zero point six seven four five, the highest in South Asia. The trajectory is not the artefact of a single administration; the through-line spans two governments of different political character.

On the connectivity side, the Maldives' international-bandwidth posture has materially changed across the 2018–2026 window.

The Maldives–Sri Lanka Cable became operational in 2021. The South East Asia–Middle East–Western Europe 6 cable landed in the Maldives via Dhiraagu in August 2024 with ready-for-service in early 2026. Ooredoo Maldives landed the PEACE (Pakistan and East Africa Connecting Europe) cable in Kulhudhuffushi. The India-Asia Express cable, a Reliance Jio system, landed in the Maldives in collaboration with Ocean Connect Maldives. The Domestic Submarine Cable of Maldives, a joint Dhiraagu and Ooredoo subsea system, lands at Hulhumalé and connects eight islands. In November 2025,

Google announced the Dhivaru cable, a Maldives–Christmas Island–Oman system with a new connectivity hub in Addu City, in partnership with Ooredoo Maldives, Dhiraagu, and the Government of Maldives.

Dhiraagu completed the rollout of high-speed fibre broadband to all inhabited islands by January 2025 — the first nationwide fibre-to-the-home network in the archipelago — operating a roughly twelve-hundred-and-fifty-kilometre domestic fibre backbone linking northern and southern regions with co-financing from the Asian Development Bank. Reported internet penetration sat at approximately eighty-five per cent of the population in late 2025, with mobile connections equivalent to roughly one hundred and forty-seven per cent of population and the majority of mobile connections on 3G, 4G, or 5G networks per DataReportal aggregation of operator and International Telecommunication Union data.

Commercial 5G is live: Dhiraagu launched in 2019; Ooredoo Maldives followed in December 2020 with Greater Malé coverage by August 2022 and a 5G AirFibre home-broadband product. Satellite-redundant connectivity is available: in August 2023 the Communications Authority of Maldives issued an Internet Service Provider licence to Starlink, the first such licence in South Asia. The Maldives Internet Exchange (MVIX), a carrier-neutral exchange in Malé, has been operational since late 2021.

These connectivity facts are load-bearing for the broader sovereign case. A jurisdiction with nationwide fibre, satellite redundancy, multiple submarine cables landing under different operators, a carrier-neutral exchange, and a population engaged with the internet at South-Asian-best penetration levels is a jurisdiction in which a verifiable-identity-and-tokenised-asset stack can be operated by domestic counterparties rather than out-of-jurisdiction, and in which on-chain attestation flows from Maldivian sensors and registries to Canton-resident contracts can be designed to operate reliably.

2. An archipelago is already a distributed system

A short architectural observation bears stating, because it reframes the question of how digitalisation composes with distributed-settlement architecture.

The Maldives is a state of approximately one thousand one hundred and ninety-two coral islands organised across twenty-six geographic atolls, administered — until the ratification of the Seventeenth Amendment to the Decentralisation Act on the first of December 2025 — through a two-tier topology of atoll councils above island councils, with the Seventeenth Amendment streamlining the legal frame under which sub-national authority is distributed.

The Maldives is, in physical and administrative form, a system whose nodes are spatially separated, jurisdictionally bounded, individually accountable, and required to act together for some categories of transaction (national budget allocations, tourism-receipts accounting, fiscal transfers) while operating independently for others (local service delivery, atoll-level administration).

The architectural concept the Maldives operationalises every day of its existence is the concept of a network of parties, each authoritative over local state, composing into a national aggregate without consolidating onto a single ledger.

A Canton participant node holds the state for the parties it hosts; uninvolved nodes do not see that state, by design — the sub-transaction privacy model enforced by the Daml engine ensures that each party sees only the projection of a multi-party transaction relevant to it.

The Global Synchronizer, run by Super Validators under two-thirds Byzantine Fault Tolerant consensus, orders encrypted messages between participant nodes without decrypting them; cross-node atomicity is delivered without cross-node state aggregation.

The model is not federation; it is not consolidation; it is *coordinated distribution*. Each node remains authoritative over its parties' state. Each node integrates with the others through the standard at the point of transaction rather than through the merging of state in a shared ledger.

The architectural alignment is consequential for the supervisory perimeter discussion. A Maldives counterparty operating a Canton participant node hosted locally occupies, in the Canton topology, the same architectural position that an atoll-level administrative authority occupies in the Maldives' physical topology: a node authoritative over local state, composing into a national-or-cross-border aggregate at the point of transaction, with the data residency, the supervisory accountability, and the operational responsibility located locally rather than aggregated upstream. The Maldives' physical configuration is not an obstacle to participation in a distributed settlement plane; it is a precise analogue of the distributional substrate that plane is built on.

3. The Boli–Tenzro–Canton stack as an architectural composition

We describe in this section the architectural composition that, in our reading, is the natural pathway for a jurisdiction in the Maldives' position to access the institutional plane of tokenised settlement.

The settlement layer is Canton. Final, irrevocable transfer of legal title and value is anchored in Daml contracts on the Canton Network. The Splice Token Standard V1 AllocationV1 primitive is the atomic delivery-versus-payment mechanism; the Global Synchronizer carries cross-application atomicity under Byzantine Fault Tolerant consensus; sub-transaction privacy is preserved by the Daml engine's stakeholder-scoped views.

The compliance and identity layer is Boli. Each instrument issued under a Boli pattern carries an associated *compliance pack* — a set of compliance modules configured by the issuing or transfer-agent party and executed at chain level on every transfer.

The identity component is the TDIP bridge — Tenzro Decentralised Identifiers under the `did:tenzro:human:{uuid}` and `did:tenzro:org:{uuid}` schemes, with selective-disclosure verifiable-credential issuance under the World Wide Web Consortium Verifiable Credentials Data Model 2.0 and Selective Disclosure JSON Web Token Verifiable Credentials patterns, anchored as Boli Credential contracts on Canton and presentable to off-Canton verifiers (a remittance corridor partner, a Mauritius custodian, a Dubai-domiciled prime broker) via the eIDAS 2.0 European Digital Identity Wallet substrate or the equivalent regional verifier surface.

The architectural property that matters is that the operational pattern of the Maldives' existing eFaas system — a high-enrolment centralised identity registry — is extended rather than replaced. The TDIP bridge is the layer that translates eFaas attestations into verifiable credentials that can present to a Canton counterparty without exposing the underlying personal data.

The orchestration layer is Tenzro's agentic runtime. Continuous asset-operations workflows — reconciliation against issuer registries, market-data monitoring, sanctions-screening pre-filtering, anti-money-laundering risk scoring, climate-finance measurement-reporting-verification evidence collection, sukuk-coupon-schedule monitoring, tokenised-re-

ceivables collection-status tracking, custody-position reporting — run on the Tenzro agentic runtime as autonomous workflows executing under DID-bound mandates.

Each mandate is a verifiable credential issued to the agent's Tenzro DID by the principal (an issuer, a transfer agent, a custodian, a supervisor) defining the scope, limits, permitted conditions, and revocation surface of the agent's authority. Mandates are revocable through Tenzro's authority-graph and revocation-tree primitives; revocation propagates as a Canton Credential-contract state change.

The agentic runtime composes upward with the deterministic Canton settlement layer through the Boli pack engine — agents *propose* actions; the Boli pack engine *evaluates* compliance rules; the AllocationV1 contract on Canton *executes* finality. This is the three-layer composition the International Monetary Fund's April 2026 *How Agentic AI Will Reshape Payments* note describes as the regulator-endorsed pattern for agentic AI in payments.

The accessibility surfaces are EVM and Solana. Canton is the canonical settlement venue. The technical substrate is the Canton Zenith Stack (a bytecode-compatible EVM execution surface and a Rust SVM execution surface running natively on Canton), Canton's `external_call` primitive for atomic interaction between Solidity contracts and Daml contracts, Circle's Cross-Chain Transfer Protocol version two for native USDC across thirteen and more chains under eight-to-twenty-second fast finality, and Chainlink's Cross-Chain Interoperability Protocol with System and Organization Controls 2 Type 2 certification for messaging across EVM and non-EVM (Solana) surfaces.

---

4. The AI integration consensus and the three-layer architecture

The architectural composition above is not a Boli innovation. It is a direct implementation of the institutional consensus on artificial-intelligence integration in payments that crystallised across the major standard-setting bodies and the International Monetary Fund in 2024–2026.

The cleanest articulation of the consensus is the International Monetary Fund's April 2026 note *How Agentic AI Will Reshape Payments*, published as IMF Note 2026/004 on the twenty-second of April 2026. The note frames payments as a three-layer composition: an upstream **intent and orchestration** layer, a deterministic **authorisation** layer, and a final **settlement** layer.

Agentic AI — encompassing reasoning, planning, search, negotiation, and multi-agent coordination — is explicitly sanctioned only in Layer 1, where its probabilistic character is acceptable because no authorisation or execution occurs at that layer.

Layer 2 is described as "strictly rules-based authorisation … accepting structured intent from Layer 1 only if it satisfies verifiable mandates, policy constraints, and regulatory checks"; the note names Agent Payments Protocol mandates as the operative mechanism, with mandates carrying scope, limits, actor identity, and permitted conditions under elliptic-curve digital-signature-algorithm-signed JSON Linked Data.

Layer 3 carries "irrevocable legal finality" through real-time gross settlement, instant-payment networks, central-bank-digital-currency platforms, and distributed-ledger-technology settlement rails; probabilistic systems are explicitly flagged as inappropriate at this layer.

The Bank for International Settlements' 2025 Annual Economic Report, Chapter III — *The next-generation monetary and financial system* — frames the same composition in different terms. Box B of the chapter, on artificial intelligence in anti-money-laundering, locates AI explicitly *outside* the settlement primitive: AI agents serve as "co-pilots" in screening, false-positive reduction, and pre-screening embedded in the payment instruction. Programmability lives in the ledger, intelligence lives above it.

The International Organization of Securities Commissions' March 2025 consultation report on artificial intelligence in capital markets (Consultation Report CR/01/2025) restates the body's six-measure framework and applies it to AI: senior-management oversight with clear accountability, testing and continuous monitoring, skills and expertise, third-party management with explicit service-level agreements, meaningful disclosure to customers and regulators, and data controls against bias.

The Financial Stability Board's November 2024 report on financial-stability implications of AI identifies four systemic vulnerabilities: third-party dependencies and service-provider concentration, market correlations and herding, cyber risk, and model risk plus data quality and governance.

The composite institutional position is unambiguous on two points relevant to the Boli–Tenzro–Canton composition. First, agentic AI belongs upstream of settlement, in an orchestration layer where its probabilistic char-

acter is acceptable because no authorisation or execution occurs there. Second, the governance burden of AI — model risk management, third-party concentration controls, accountability frameworks, disclosure obligations — attaches to the firm operating the model and does not migrate into the deterministic smart-contract layer beneath it.

Three integration mechanisms warrant brief description because they carry the load of the Layer-1-to-Layer-2 handoff.

DID-bound mandates. Each Tenzro-runtime agent operates under a verifiable-credential mandate issued by the principal — a transfer agent, a custodian, an issuer, a supervisor — to the agent's TDIP-anchored decentralised identifier.

The mandate is a JSON Linked Data document, signed by the principal's elliptic-curve key, carrying the scope (which assets, which actions, which jurisdictions), the limits (transaction sizes, frequency caps, drawdown bounds), the actor identity (the agent's DID), and the permitted conditions (which compliance attestations must be present, which counterparty types are permitted).

The World Wide Web Consortium's Agent Identity Registry Protocol Community Group (established April 2026) and the OpenID Foundation's Artificial Intelligence Identity Management Community Group are converging on the standard format; the Decentralized Identity Foundation received the Model Context Protocol Identity specification donation in March 2026. The pattern is established; the standardisation is in progress.

Trusted Execution Environment attestation for agent compute. Agentic AI inference in the Tenzro runtime runs in Trusted Execution Environments — composite Intel Trust Domain Extensions plus NVIDIA H100 attestation via Intel Trust Authority is the production-ready pattern in 2026, with Advanced Micro Devices' Secure Encrypted Virtualisation–Secure Nested Paging, Amazon Web Services' Nitro Enclaves, and Google Cloud Platform's Confidential Space as alternative substrates. Each inference is bound to an attestation report demonstrating *what code ran on what input.* The honest caveat: verifiable compute proves what code ran, not that the model's output is correct.

Authority graphs and revocation trees. Mandates compose into authority graphs — chains of delegation from a principal to a sub-agent to a sub-sub-agent, each link a verifiable credential — and the revocation of any link propagates through the tree. The architectural property is that an autonomous workflow's authority can be revoked at any layer of the delegation chain without bringing down the workflow itself.

5. Sovereign AI, air-gapped AI, and the decentralised-compute marketplace

The agentic-finance layer surfaced above as the upstream orchestration layer in the three-layer architecture is, in 2025–2026, no longer a research category. Google's Agent Payments Protocol launched on the sixteenth of September 2025 with sixty-plus partners — American Express, Coinbase, Etsy, Intuit, Mastercard, PayPal, Salesforce, ServiceNow, Adyen, MetaMask, Revolut, Worldpay, and others — and was donated to the FIDO Alliance on the twenty-eighth of April 2026. Mastercard contributed a complementary standard called Verifiable Intent (a tamper-proof log of user-authorised agent actions) to the same FIDO process.

Coinbase's x402 — the open Hypertext Transfer Protocol payment standard using the four-hundred-and-two Payment Required status code — had by the first quarter of 2026 processed approximately one hundred and nineteen million transactions on Base and thirty-five million on Solana, with roughly six hundred million dollars in annualised payment volume. The x402 Foundation was announced jointly by Cloudflare and Coinbase on the twenty-fifth of September 2025; the Solana Foundation joined under a Linux Foundation umbrella, and Stellar added support, in April 2026.

Mastercard launched **Agent Pay** on the twenty-ninth of April 2025, with Agentic Tokens piloted with Citi and U.S. Bank in September 2025 and extended to all United States cardholders in November 2025. Visa launched **Intelligent Commerce** earlier in 2025 and reported, on the eighteenth of December 2025, that the programme had completed hundreds of agent-initiated transactions in production environments.

Visa joined Canton as a Super Validator on the twenty-fifth of March 2026 as the first major global payments company in the role and at the highest Super Validator weight in the network, which places the agentic-commerce position and the tokenised-settlement position inside a single corporate posture.

The IMF Note of the twenty-second of April 2026 reads the situation as a movement from Know-Your-Customer toward **Know-Your-Agent** — mandated verifiable identities for financial bots linked to legal entities, with human-in-the-loop safeguards, real-time anomaly monitoring, and audit-grade activity logs as the standing supervisory requirements.

Beneath the protocol record sits the supervisory frame. The Financial Stability Board has repeatedly named — in the November 2024 *Financial Stability Implications of Artificial Intelligence* and the October 2025 monitoring report — **third-party dependency** on a small number of artificial-intelligence service providers as a systemic concern for the financial sector.

The concentration of inference and model-hosting capacity in a handful of hyperscale cloud providers and frontier-model laboratories is the structural property the supervisory bodies have flagged.

The standard agentic-finance compositions described above sit on top of that concentrated provider set: when an agentic-payment platform calls a model, the call typically goes to one of a small number of hosted endpoints; when the compliance pack on a Canton contract evaluates an agent's mandate, the agent's underlying inference often ran inside a Trusted Execution Environment on a hyperscaler's hardware. The Trusted Execution Environment attestation closes the integrity question — proving the claimed code ran on the claimed inputs — but it does not close the concentration question.

The Tenzro Network is, by construction, the decentralised-compute response to that concern. It is an open-source compute marketplace in which agents discover and pay for inference, training, and general compute resources directly within the network, without routing through centralised provider intermediation.

The provider set is open: independent node operators and small-to-medium data centres operate as providers within the network on equal protocol footing with larger operators.

Trusted Execution Environment attestation (composite Intel Trust Domain Extensions plus NVIDIA H100 or H200 attestation; AMD Secure Encrypted Virtualisation with Secure Nested Paging; Amazon Web Services Nitro Enclaves; Google Cloud Confidential Space) is supported across the provider population; agents present signed mandates under their decentralised identifiers and pay for inference in cleared settlement assets at the protocol layer.

The economic structure dissolves the toll-collector position that the hyperscale-and-frontier-laboratory configuration concentrates; the supervisory structure dissolves the third-party-dependency concern that the Financial Stability Board has named.

A second property follows. **Tenzro supports air-gapped artificial-intelligence model deployment on the same protocol surface** — model and inference workload running inside a closed compute bound-

ary, with no traffic leaving that boundary to a hyperscale provider, while the attestation pipeline still proves to a regulator or to an asset-contract compliance pack that the claimed code ran on the claimed input.

The composition has direct supervisory implications. A central bank running sanctions-screening or anti-money-laundering inference can do so without sending payloads to a foreign-jurisdiction hyperscaler; a sovereign issuer running model-assisted disclosure preparation can keep the disclosure inside a closed compute boundary until release; **a Maldivian regulator can keep regulated-entity inference inside a Maldivian or trusted-jurisdiction compute footprint, with attested verifiability to the supervisor without data exfiltration.**

The data-sovereignty objection that has slowed sovereign and bank-side artificial-intelligence adoption through 2024 and 2025 is, in this configuration, addressable rather than deferred.

The full agentic-finance pipeline that crystallises in 2026 is therefore the following composition: the agent runs inside a Trusted Execution Environment that produces a composite Intel Trust Domain Extensions plus NVIDIA attestation; the provider hosting the Trusted Execution Environment is one of many independent node operators or data-centre operators within the Tenzro Network rather than a single hyperscale provider; the agent holds a decentralised identifier and a verifiable mandate from the customer (under Agent Payments Protocol or Model Context Protocol Identity); the agent forms intent and signs an intent message under that mandate; for settlement on Canton, the Boli compliance pack on the asset contract verifies the mandate signature, the mandate freshness, the counterparty eligibility, and (where required) the attestation evidence; the atomic delivery-versus-payment primitive executes the asset and cash transfers in a single Daml transaction.

The Trusted Execution Environment closes integrity; the decentralised provider set closes concentration; air-gapped deployment closes data-sovereignty; the compliance pack closes regulatory eligibility; the atomic settlement primitive closes finality.

The architecture of agentic finance that the International Monetary Fund, the Bank for International Settlements, the International Organization of Securities Commissions, and the Financial Stability Board have collectively endorsed in 2025–2026 is realised on this composition without the concentration risks the same bodies have flagged.

For the Maldives, the practical reading is that agentic finance is not a long-horizon question — the institutional adoption is happening through 2026 — and that the architectural posture available to the jurisdiction is one in which the compute layer underneath the agent is decentralised by construction rather than dependent on a single foreign provider.

6. Security: the 2026 institutional norm

The architectural composition inherits the security primitives of three layers — Canton, Boli, Tenzro — each with its own evolving institutional norm.

Threshold-signing and the multi-party-computation wallet substrate. The 2026 institutional norm has settled on threshold multi-party-computation over multi-signature for digital-asset key management, with the Gennaro-Goldfeder 2020 protocol dominant on account-based EVM and SVM chains and FROST — the Flexible Round-Optimised Schnorr Threshold protocol, standardised as Internet Engineering Task Force Request for Comments 9591 in 2024 — the institutional choice for Schnorr and Taproot signatures, Ed25519 signatures, and Canton-aligned signing curves.

The Boli–Tenzro pattern of multi-party-computation wallets bound to TDIP decentralised identifiers across the secp256k1, ed25519, and Canton signing curves is consistent with the FROST and Gennaro-Goldfeder primitives. The architectural property is that a Maldives Monetary Authority decentralised identifier — or a Maldives International Financial Services Authority licensee's decentralised identifier — can hold signing authority across Ethereum, Solana, and Canton through a single TDIP-anchored key arrangement rather than across three separately-managed custody relationships.

Trusted Execution Environment attestation for validator and agent compute. The 2026 hardware substrate is Intel Trust Domain Extensions, Advanced Micro Devices' Secure Encrypted Virtualisation–Secure Nested Paging, NVIDIA H100, H200, and B200 confidential compute, Amazon Web Services' Nitro Enclaves, and Google Cloud Platform's Confidential Space.

Composite attestation — Intel Trust Domain Extensions plus NVIDIA H100 — moved from preview to general availability via Intel Trust Authority during 2025, on Ubuntu 24.04 long-term-support and Linux kernel 6.8 and above. NVIDIA confidential graphics processing units with encrypted video memory are deployed in regulated inference workloads.

For the Boli–Tenzro composition the relevant production application is Layer-1 agentic inference: each inference an agent produces is bound to a Trusted Execution Environment attestation report, presentable to a supervisor as evidence of *what code ran on what input*, with the caveat that this is not evidence of model-output correctness.

Post-quantum cryptography. The National Institute of Standards and Technology finalised the principal three post-quantum cryptographic standards in August 2024 — Federal Information Processing Standards Publication 203 (Module-Lattice-Based Key-Encapsulation Mechanism, formerly CRYSTALS-Kyber), 204 (Module-Lattice-Based Digital Signature Algorithm, formerly Dilithium), and 205 (Stateless Hash-Based Digital Signature Algorithm, formerly SPHINCS+) — with Federal Information Processing Standards Publication 206 (FN-DSA, formerly Falcon) in draft.

National Institute of Standards and Technology Internal Report 8547 proposes deprecating Rivest-Shamir-Adleman and Elliptic Curve Cryptography at 112-bit security after 2030, with all quantum-vulnerable asymmetric cryptography disallowed after 2035. No major Layer 1 blockchain — Canton included — has rotated its base signature scheme to post-quantum cryptography. The Group of Seven Cyber Expert Group's January 2026 roadmap targets 2030 to 2032 for critical financial-system migration. For the Boli–Tenzro–Canton stack the relevant 2026 architectural requirement is crypto-agility — the ability to rotate signature schemes without protocol forks — rather than immediate post-quantum deployment.

7. Privacy: Canton's sub-transaction model and the verifiable-credential substrate

The privacy guarantees of the Canton settlement layer are the architectural property most directly relevant to a sovereign or sovereign-adjacent participant.

Canton implements **SUB-TRANSACTION PRIVACY** through stakeholder-scoped views: each participant node receives only the projection — the sub-transaction — of a multi-party transaction relevant to the parties it hosts. Uninvolved nodes never see or process confidential portions of the transaction. This is enforced cryptographically by the Daml engine, not by ledger policy.

The mechanism is materially different from public-permissioned chains running Hyperledger Besu Istanbul Byzantine Fault Tolerance, where validators see plaintext, and from Layer 2 rollups, where the sequencer sees full state.

The Global Synchronizer, operated by Super Validators under two-thirds Byzantine Fault Tolerant consensus, sequences *encrypted* messages, runs consensus on ordering, and guarantees that multi-leg transactions either fully succeed or fully fail — without decrypting payloads at any point.

A Daml contract is a multi-party agreement whose stakeholders are formally classified as signatories (who must authorise the contract's creation and consume), observers (who see the contract but cannot exercise choices on it), controllers (who exercise choices), and informees (who see particular sub-transaction projections by virtue of their roles in particular choices).

The Daml engine computes a separate *projection* of any multi-party transaction for each participant node, including only the sub-transactions in which the parties hosted on that node are stakeholders. Uninvolved participant nodes receive nothing — not an encrypted ciphertext, not a hash, not a transaction identifier.

Each participant node maintains a private database holding only the projections relevant to the parties it hosts; the Global Synchronizer routes encrypted, addressed messages between participants and orders them under Byzantine Fault Tolerant consensus, but the Synchronizer's Super Validators never decrypt payloads and do not have read access to participant-node private databases.

The supervisory pattern that follows from the model is *regulator-as-observer*: a supervisor with statutory access to a class of contracts is permissioned as a Daml observer party on the relevant templates, receives the projection containing exactly the data the licence requires, and is precluded by the engine's projection logic from receiving anything outside that scope.

The privacy substrate above Canton — the verifiable-credential layer carrying identity, attestation, and authorisation data — has settled on three primary standards. The World Wide Web Consortium's Verifiable Credentials Data Model 2.0 became a Recommendation on the fifteenth of May 2025.

The 2026 institutional stack composes three credential formats: Selective Disclosure JSON Web Token Verifiable Credentials, mandated alongside Mobile Document under the European Union's eIDAS 2.0 European Digital Identity Wallet programme and the dominant choice for institutional Know-Your-Customer-tier disclosure; Boneh-Boyen-Shacham signatures under the `bbs-2023` cryptographic suite, providing unlinkable selective disclosure with one issuer signature and multiple holder-derived proofs (the strongest privacy properties, with heavier cryptography); and the Mobile Document standard under International Organization for Standardization 18013-5, mandated for mobile driving licence and co-mandated alongside Selective Disclosure JSON Web Token Verifiable Credentials under eIDAS 2.0.

Sovereign data residency and digital sovereignty bear on any Canton participation by a Maldives-domiciled supervisor. The relevant frameworks include the European Union's General Data Protection Regulation Article 48 (third-country authority data requests inadmissible without European Union legal basis), the European Union Data Act in force since 2025 (cloud-portability and non-personal-data rules), India's Digital Personal Data Protection Act 2023, Singapore's Personal Data Protection Act, and the Maldives' own regime.

The operative Maldives regime in May 2026 is the 2017 Data Protection Act plus the direction of travel in the Privacy and Personal Data Protection Bill, drafted in 2023 and in active legislative process through 2025 — the Bill creates a dedicated data-protection authority and is European-Union-General-Data-Protection-Regulation-aligned but had not been enacted as of the eleventh of May 2026.

The constraint on Canton participation flows from the architecture rather than the legal text: Canton's privacy model means contract content does not leave participant nodes the sovereign controls; the cross-jurisdictional exposure is via the Super Validator operators (currently non-Maldives), any Boli-hosted off-ledger components, and the settlement-asset issuers' nodes.

A sovereign Maldives participant node, operated locally on Tenzro infrastructure, satisfies data-residency for state-held contract data; the Global Synchronizer sees no plaintext, which is the architectural property that makes Canton tractable for sovereign participation under General-Data-Protection-Regulation-class regimes.

8. Interoperability: multi-virtual-machine accessibility, settlement-asset agnosticism

The interoperability properties of the Boli–Tenzro–Canton composition derive from three architectural decisions.

Canton as canonical settlement, EVM and Solana as accessibility surfaces. Canton's `external_call` primitive enables atomic interaction between Solidity contracts and Daml contracts — a Solidity contract on Ethereum or an Ethereum Layer 2 can invoke a Daml contract on Canton within the same transaction, with finality preserved by the Daml engine.

Canton's Zenith Stack — a bytecode-compatible Zenith Ethereum Virtual Machine execution surface and a Rust Solana Virtual Machine execution surface running natively on Canton — exposes the Canton ledger to Ethereum-resident and Solana-resident wallets without requiring custodial bridges.

Cross-chain messaging via Circle's Cross-Chain Transfer Protocol version two (live for native USDC across thirteen chains and counting, with eight-to-twenty-second fast finality and zero peg risk because the underlying USDC is burnt on the source and minted on the destination) and Chainlink's Cross-Chain Interoperability Protocol (carrying multi-chain messaging including USDC under Cross-Chain Transfer Protocol version two, with System and Organization Controls 2 Type 2 certification — the only blockchain protocol so certified — and processing four-hundred-billion-dollar transaction volumes in 2025 and 2026) completes the multi-chain access pattern.

Settlement-asset agnosticism. The AllocationV1 primitive does not bind to a particular cash token: it consumes whatever cleared payment-asset the counterparties have agreed on at the transaction layer. The set of cleared payment-assets that compose against AllocationV1 in 2026 includes regulated dollar stablecoins (Circle USDC, Paxos USDP, the GENIUS-Act-compliant universe), tokenised money-market funds (Hashnote USYC, BlackRock BUIDL, Franklin Templeton's FOBXX), tokenised bank deposits (JPMorgan JPMD, Bank of New York Mellon's institutional deposit token, Standard Chartered's tokenised deposits, DBS Token Services), and — as

central-bank programmes mature — wholesale central-bank digital currencies on the Project Helvetia, Project Pontes, Project Ensemble, and mBridge surfaces.

The strategic implication is that the choice of settlement asset is a counterparty-and-regime question, not a platform question.

---

9. The architecture against the Maldives' empirical record

A useful comparator, visible in the public record, is the architectural posture taken by foreign-capital projects already operating in the Maldives' digital-asset perimeter.

The Trump Organization's Trump International Hotel Maldives project, announced on the seventeenth of November 2025 in partnership with Dar Global as a roughly three-hundred-million-dollar branded resort development, is the most publicly visible foreign-capital tourism engagement of the current cycle.

In a separate but architecturally telling development, on the eighteenth of February 2026 Dar Global announced — in partnership with World Liberty Financial and Securitize — a tokenisation programme covering loan-revenue interests in a Dar Global property portfolio, structured for distribution to United States accredited investors under Rule 506(c) of Regulation D and to non-United-States investors under Regulation S, with on-chain mechanics implemented on the Morpho protocol on the Base Ethereum Layer 2.

The architectural posture of the Dar Global / World Liberty Financial / Securitize transaction is the opposite of the institutional Canton plane in three respects: the chain is public Ethereum Layer 2 rather than a privacy-preserving permissioned ledger; the asset is debt-side loan-revenue interests rather than a tokenised equity or settlement instrument; and the investor surface is accredited-only retail distribution rather than central-bank- and Super-Validator-mediated wholesale settlement.

The comparator matters because it shows that tokenisation interacting with the Maldives' surface is already happening on a substantively different architectural plane from the one described in this paper, and that the choice of plane carries direct consequences for supervisory perimeter, counterparty composition, and the residual exposure the Maldives' state retains.

10. The risk posture and the asymmetry of the pathway

The extract closes by setting out what is uncertain about the digitalisation environment around the architectural pathway, and how the pathway composes with that uncertainty. The architectural pathway is built so that the residual question it leaves with the Maldivian state is a question of pace and posture, not of architectural irreversibility.

A preliminary observation bears stating. The conservative posture in the Maldives' present configuration is not the do-nothing posture. The do-nothing posture is the posture in which agentic-finance and tokenisation interacting with the Maldives' surface continues to happen on architectural planes the Maldivian state has no supervisory grip on — public-permissionless Ethereum Layer 2 distribution, foreign-hyperscaler AI inference under no domestic data-residency guarantee, decentralised-identifier-bound agent mandates issued out-of-jurisdiction. Doing nothing concedes the digitalisation ground to those pathways. The conservative posture is the posture that establishes the supervisory perimeter and the digitalisation surface within which subsequent decisions are taken.

10.1 The talent-and-execution capacity the pathway requires

The first surface concerns whether the Maldives possesses the digital-engineering capacity the pathway requires. The Maldives' digital-government and digital-finance work to date — eFaas, OneGov, Favara, Bandeyri, Beelan, Neelan, the Bank of Maldives Swipe wallet — has been built by the National Centre for Information Technology and the Maldives Monetary Authority in collaboration with international technology partners: Tietoevry (Finland) for Favara, NPCI International (India) for the Unified Payments Interface integration, Mastercard (from October 2025) for the Digital Country Partnership and the Smart-ID rollout. The partner-with-an-international-technology-provider pattern is institutionalised in Maldivian digital-government delivery; it is not a new posture being introduced.

The Boli–Tenzro–Canton pathway is consistent with that established pattern. Tenzro Labs Pte. Ltd. (Singapore) is the engineering partner for the validator-node, runtime, and decentralised-compute layer, on the same architectural footing the Maldives' existing technology partners occupy in

their respective layers. The Boli platform's open-source Daml pattern library and compliance-pack catalogue are accredited-counsel-authorable across Maldivian, Mauritian, Gulf, and Singapore-aligned regimes; the engineering build does not require resident Daml capacity in the Maldives in year one or year two.

Regional capacity matters here. Mauritius, Seychelles, and Singapore have measurably higher digital-finance institutional density than the Maldives does as of 2026, and each is a plausible source of pooled regional engineering capacity — Mauritius under its Virtual Asset and Initial Token Offering Services regime, Singapore under the Monetary Authority of Singapore's Project Guardian, Seychelles under the Financial Services Authority's digital-asset framework. The architectural pathway composes with regional-capacity pooling; it composes with hosted-by-Tenzro-Labs-from-Singapore operation; it composes with the Maldives growing resident capacity over a multi-year horizon. None of those three patterns is dependent on either of the others.

The capacity question is therefore a sequencing question, not an irreducible obstacle. The Maldives' choice of whether to build capacity domestically, to pool regionally, or to procure internationally is preserved at the institutional layer where it conventionally sits, on the timeline the supervisory authority chooses.

10.2 Data sovereignty under an evolving Maldivian regime

The second surface concerns data sovereignty under a Maldivian regulatory regime that is itself in formation. The operative Maldives regime in May 2026 is the 2017 Data Protection Act plus the direction of travel in the Privacy and Personal Data Protection Bill, drafted in 2023 and in active legislative process through 2025 — the Bill creates a dedicated data-protection authority and is European-Union-General-Data-Protection-Regulation-aligned but had not been enacted as of the eleventh of May 2026.

The architectural properties that bear on the risk posture are three. **Canton's sub-transaction privacy model** means contract content does not leave participant nodes the Maldives' supervisor controls; a sovereign Maldives participant node, operated locally on Tenzro infrastructure, satisfies data-residency for state-held contract data, and the Global Synchronizer's Super Validators never decrypt payloads. **Tenzro's decentralised-compute marketplace and air-gapped AI deployment** allow regulated-entity inference to run inside a Maldivian or trusted-jurisdiction compute footprint, with attested verifiability to the supervisor and no data exfiltration to a foreign-jurisdiction hyperscaler. **Verifiable credentials with selective disclosure** under the W3C Verifiable Credentials Data Mod-

el 2.0 and the Selective Disclosure JSON Web Token Verifiable Credentials format mean cross-border Know-Your-Customer attestations present without disclosing the underlying personal data the Maldivian regime would protect.

The architectural pathway is therefore consistent with the 2017 Act today, consistent with the Privacy and Personal Data Protection Bill when enacted, and consistent with any reasonable subsequent tightening of the regime. The data-residency posture is set by the deployment topology, not by the platform substrate; the platform substrate composes with strict-residency, regional-pooling, and hybrid postures.

10.3 The standards work that closes the remaining architectural gaps

The third surface concerns the standards work that closes the remaining architectural gaps. The gaps surfaced in this extract — the standardisation of decentralised-identifier-bound artificial-intelligence mandates and revocation trees, the supervisory recognition of Trusted Execution Environment-attested agent compute, the post-quantum-cryptography migration trajectory for Canton signing curves, the eIDAS 2.0 mutual-recognition pathway for non-European-Union national-identity schemes including eFaas — are real, and each is a standards-body workstream of broader relevance.

The architectural property that bears on the risk posture is that none of those gaps is the Maldives' alone to close. The World Wide Web Consortium, the Fast Identity Online Alliance, the Decentralised Identity Foundation, the OpenID Foundation, the Internet Engineering Task Force, the International Organization for Standardization, and the Bank for International Settlements' Innovation Hub are the bodies in which these workstreams sit. The Boli Standards Proposals series is the editorial vehicle through which the Boli Association contributes to those workstreams.

The Maldives' configuration choices in the 2026–2028 window do not require the gaps to be closed before participation. The pathway composes with the gaps as they are closed; the gaps as they exist today do not block an eFaas-to-TDIP credential bridge, do not block a Tenzro-hosted air-gapped inference deployment for a Maldivian regulator, and do not block the Centre's bespoke regime adopting verifiable-credential substrates for participant accreditation. The standards trajectory and the Maldives' decision horizon are independent variables; the architecture is designed so that they remain independent.

10.4 The asymmetry

The structural property the three sub-sections above share is asymmetry. Under each surface of uncertainty, the residual exposure of the pathway is bounded by the platform substrate being open source and shipping today, by Canton's sub-transaction privacy enforcing data residency at the architectural layer, by Tenzro's decentralised-compute marketplace and air-gapped AI deployment dissolving the hyperscaler concentration concern, by verifiable-credential selective disclosure preserving personal-data protection across borders, and by the standards trajectory being a broader workstream the Maldives joins rather than carries.

The architectural pathway described exists in 2026 — built on shipped, open-source software at the Canton, Splice, and Boli layers; on production Trusted Execution Environment attestation primitives at the Tenzro orchestration layer; on the regulator-endorsed three-layer composition for agentic artificial intelligence; and on the verifiable-credential, multi-party-computation, and post-quantum-migration substrates the institutional financial system has settled on.

The question the architecture leaves with the Maldivian state is a question of pace and posture, not of architectural irreversibility. The choice of whether to enter the digitalisation venue as an early-acting jurisdiction — eFaas-to-TDIP credential bridge, regulator-operated participant node, air-gapped AI inference within a Maldivian compute footprint — or to engage the pathway later through Centre-licensed counterparties, or to defer the choice further, remains a sovereign one. The architectural ground on which the choice is made, however, exists today and is consistent with each of those postures.