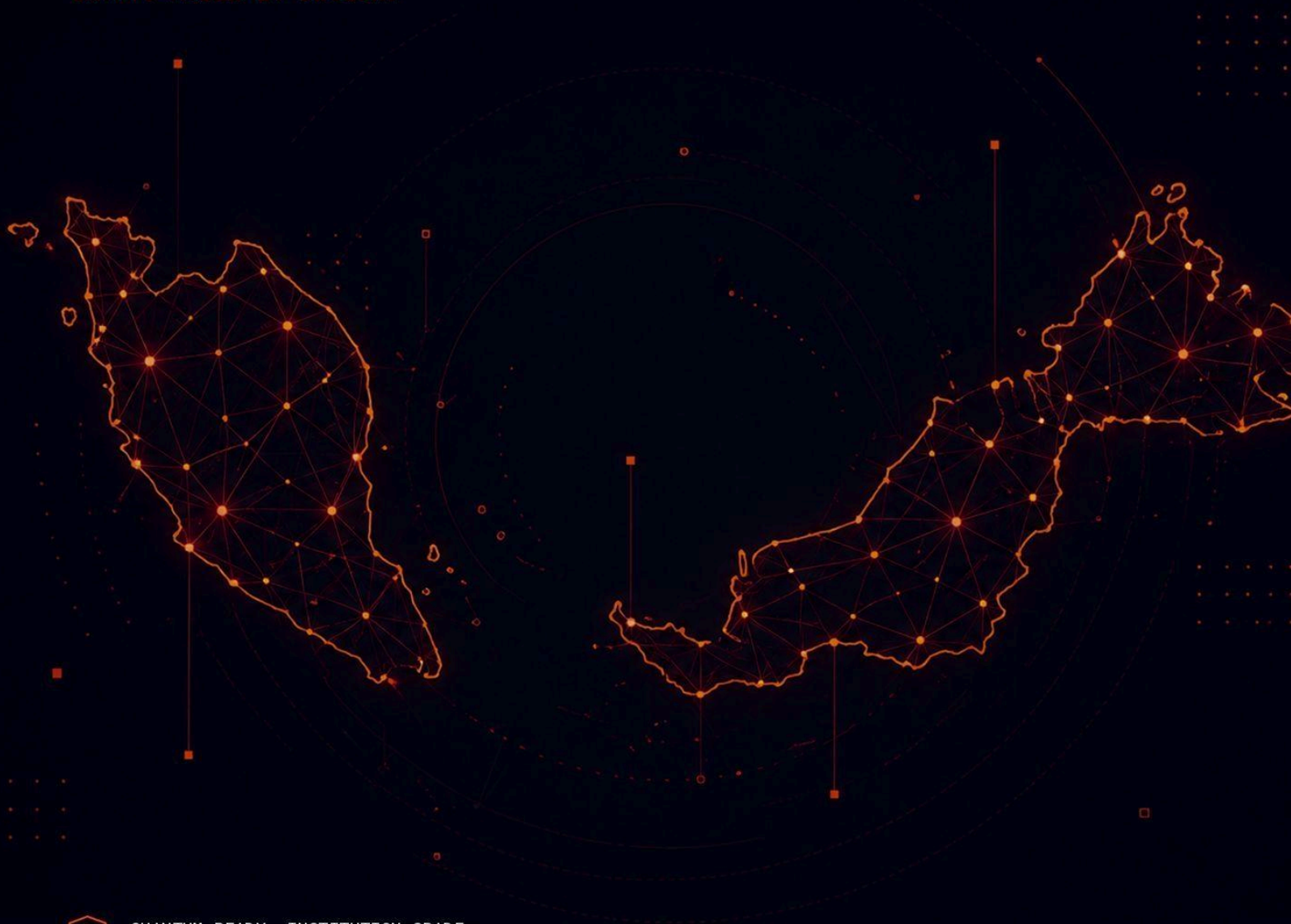




# Merdeka : A Malaysian Quantum-Ready Layer-1 Blockchain Purpose-Built For Institutional Finance

SOVEREIGN INFRASTRUCTURE.  
CRYPTO-AGILE BY DESIGN.



QUANTUM-READY. INSTITUTION-GRADE.  
BUILT FOR MALAYSIA.

# MerdekaL1: A Malaysian Quantum-Ready Layer-1 Blockchain Purpose-Built For Institutional Finance

OCTOBER 2026

|               |                                                          |
|---------------|----------------------------------------------------------|
| Ee Wui Yang   | <a href="mailto:wuiyang.ee@e23.io">wuiyang.ee@e23.io</a> |
| Tan Yen Khoon | <a href="mailto:yk@e23.io">yk@e23.io</a>                 |
| Stanly Hor    | <a href="mailto:stanly@e23.io">stanly@e23.io</a>         |
| Rachel Yue    | <a href="mailto:rachel.yue@e23.io">rachel.yue@e23.io</a> |

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>ABSTRACT</b>                                               | <b>1</b>  |
| <b>1 / INTRODUCTION</b>                                       | <b>2</b>  |
| <b>2 / CORE ARCHITECTURE OF THE NETWORK</b>                   | <b>4</b>  |
| <b>3 / GOVERNANCE OF QUANTUM-READY DIGITAL INFRASTRUCTURE</b> | <b>9</b>  |
| <b>4 / USE CASE: INVOICE LIFECYCLE INFRASTRUCTURE</b>         | <b>13</b> |
| <b>5 / CURRENT PROGRESS AND ROADMAP</b>                       | <b>15</b> |
| <b>6 / WHAT e23 BRINGS TO THE TASKFORCE</b>                   | <b>16</b> |
| <b>7 / CONCLUSION</b>                                         | <b>17</b> |
| <b>REFERENCES</b>                                             | <b>18</b> |
| <b>TECHNICAL APPENDIX</b>                                     | <b>19</b> |
| <b>DISCLAIMER</b>                                             | <b>20</b> |

**ABSTRACT**

MerdekaL1 is a purpose-built, EVM-compatible Layer-1 blockchain for Malaysia's digital economy and institutional finance. Cryptographic agility is its foundational design principle: the governance layer is designed to support the substitution of algorithms, keys and signing primitives without network disruption, chain restarts or asset migration. Its hybrid signing architecture reserves high-security institutional operations, including governance and high-value transactions, for a validated post-quantum signature scheme, while ECDSA supports general-purpose transactions within protocol-level spend limits. The WalletSymlink dual-identity model unifies these roles within a layered security strategy. The network combines this architecture with deterministic settlement finality through the MERDEKA Byzantine Fault Tolerant (BFT) consensus engine, a multi-authority governance framework anchored by the MERDEKA Security Council, and a governed execution environment supporting identity-linked participation, programmable compliance and private permissioned access. MerdekaL1 is designed and built in Malaysia, and is positioned as shared digital infrastructure on which regulated institutions, public-sector systems and developers can build.

## 1 / INTRODUCTION

Critical digital infrastructure is being built today on cryptography that will not remain secure for the full lifetime of the assets and records it protects. Malaysia's digital economy faces three structural conditions that current public blockchain infrastructure was not designed to address.

The first is the cryptographic obsolescence horizon. The cryptography that secures every major public blockchain in production today depends on the discrete logarithm problem on elliptic curves, which is solvable in polynomial time on a sufficiently large quantum computer running Shor's algorithm (Shor, 1994). The United States National Institute of Standards and Technology finalised the first post-quantum cryptographic standards in August 2024 (NIST, 2024a, 2024b, 2024c), and the G7 Cyber Expert Group has called for a coordinated roadmap for the financial sector's transition to post-quantum cryptography (G7 Cyber Expert Group, 2026). Recent reductions in the qubit estimates required to break elliptic curve cryptography at currently deployed parameter sizes have continued to narrow the defensible planning horizon for institutions holding long-duration assets (Google Quantum AI, 2026). Malaysia has set its own national direction. The National Cyber Security Agency issued the National PQC Readiness Roadmap in October 2025, initiating PQC migration across National Critical Information Infrastructure (NCII) sectors (NACSA, 2025), and CyberSecurity Malaysia has published complementary guidance on cryptographic agility and quantum-safe adoption (CyberSecurity Malaysia, 2025).

The second is the domestic infrastructure gap. Malaysia's ambitions for its digital economy and capital market increasingly depend on programmable, verifiable digital infrastructure. The Securities Commission Malaysia's Capital Market Masterplan 2026–2030 projects a capital market of RM5.8 to RM6.3 trillion by 2030 and RM13.8 to RM20 trillion by 2045, and directs capital towards high-growth sectors including the digital economy (Securities Commission Malaysia, 2026). Infrastructure supporting that growth must be governable by domestic authorities and institutions under Malaysian jurisdiction. Permissionless smart contract chains accept the regulatory ambiguity that comes with open validator participation. Closed consortium chains sacrifice the developer ecosystem and interoperability that make public chains useful infrastructure. Neither category satisfies the brief.

The third is the governance and agility requirement. Quantum readiness requires institutions to govern how cryptographic algorithms are selected, validated, deployed and replaced. Experience across the post-quantum field has shown that candidate schemes can be weakened or broken by

new cryptanalysis after publication, so infrastructure that depends on any single primitive inherits that risk. Long-lived infrastructure must therefore support changes to keys and signing primitives as quantum threats, cryptanalysis and recognised standards evolve, without network disruption or migration of the underlying assets. Clear institutional authority, decision rights and accountability are what make that capability auditable and durable.

This litepaper introduces MerdekaL1. The architecture rests on the position that national digital infrastructure must be cryptographically durable, regulatorily native and institutionally governable from the protocol level upward. MerdekaL1 introduces three core innovations:

1. **Hybrid Signing and Cryptographic Agility at the Protocol Level:** MerdekaL1 is designed to support governed substitution of algorithms, keys and signing primitives while preserving network continuity. Its hybrid model assigns high-security institutional operations, governance and high-value transactions to a post-quantum signing layer, and general-purpose transactions to ECDSA within protocol-level spend limits. WalletSymLink connects each participant's primary post-quantum identity with an EVM alias. The architecture does not depend on any single post-quantum primitive: the production scheme is selected, validated and, where required, replaced through the governance process, with reference to NIST standards and CyberSecurity Malaysia's MySEAL framework.
2. **MERDEKA Consensus and Institutional Governance:** MERDEKA targets sub-2-second deterministic finality with a planned validator set of 20 to 30 institutional participants drawn from across the financial, cybersecurity, regulated industry and government domains. A planned Security Council is designed to hold authority over validator admission, protocol parameters and emergency response, separating technical block production from institutional decision-making.
3. **Governed Execution Environment:** MerdekaL1 is EVM-compatible, with native protocol-level controls for identity-linked participation, programmable compliance and private permissioned access, so that applications inherit institutional requirements rather than reconstructing them.

These innovations are integrated rather than isolated. Together they define what national digital infrastructure must be to remain credible across the cryptographic, regulatory and institutional horizons of the next decade.

## 2 / CORE ARCHITECTURE OF THE NETWORK

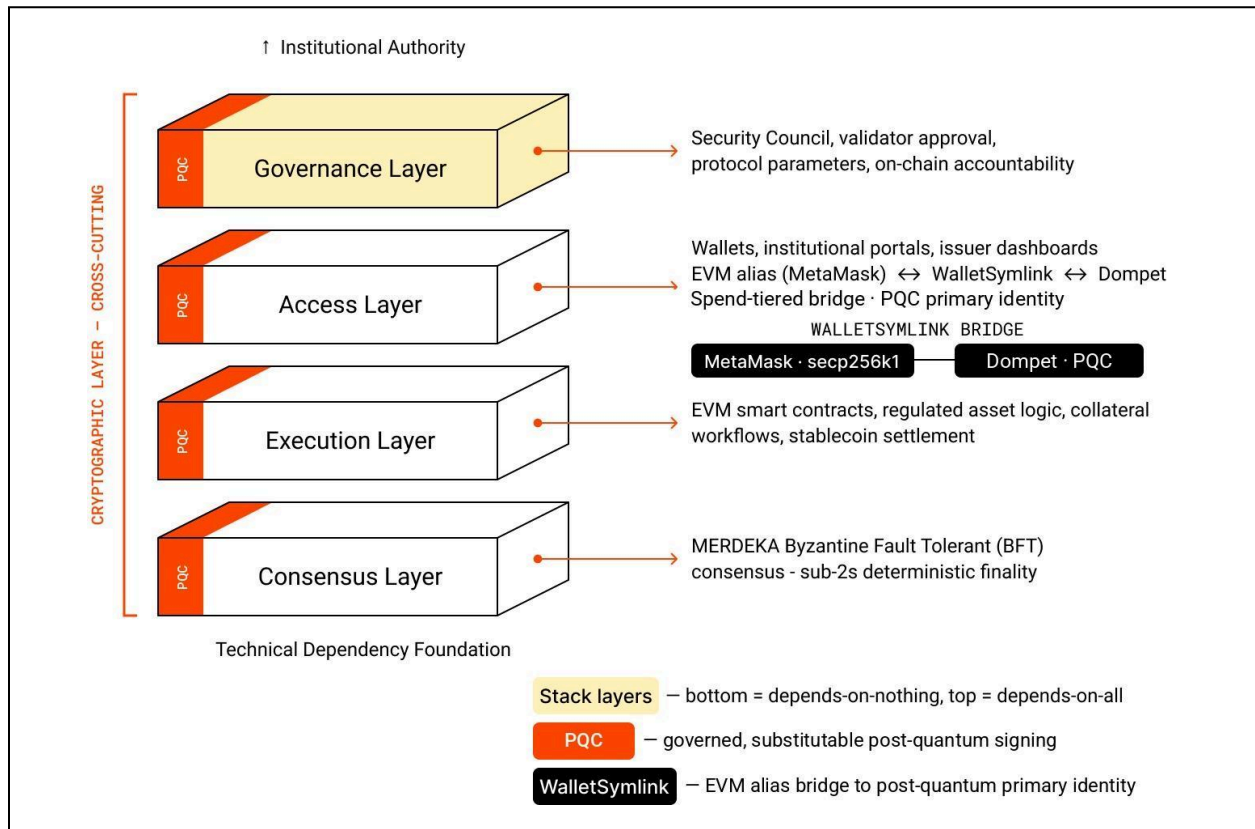


Figure 1: Four layers of architecture on the network

The architecture of MerdekaL1 is structured across four layers. From the ground up, the Consensus Layer covers MERDEKA Byzantine Fault Tolerant (BFT) consensus. The Execution Layer covers EVM smart contracts, regulated asset logic and settlement workflows. The Access Layer covers wallets, institutional portals and issuer dashboards, supporting EVM-compatible wallet access, including MetaMask and other standard interfaces, alongside WalletSymLink integrations such as Dompot for identity-linked and institution-aligned participation. The Governance Layer covers Security Council oversight, validator approval, protocol parameter control and on-chain accountability.

Three foundational pillars structure the design, with governance treated as a standalone discussion in Section 3:

- Hybrid signing and governed cryptographic agility align transaction permissions with institutional risk and support cryptographic renewal over the life of an asset or record;
- MERDEKA consensus provides deterministic settlement finality with institutional accountability; and

- The governed execution environment provides the controls institutional workflows require, embedded at the protocol level rather than reconstructed by every application.

## // 2.1 HYBRID SIGNING AND CRYPTOGRAPHIC AGILITY

Cryptographic agility leads to MerdekaL1's security architecture. The protocol is designed to substitute algorithms, keys and signing primitives through governance without network disruption, chain restarts or asset migration. Its hybrid model gives a post-quantum signing layer and ECDSA distinct, complementary roles within one security strategy, combining quantum readiness, controlled transaction authority and EVM interoperability.

**Complementary signing roles within a unified architecture.** The post-quantum signing layer is designated for high-security institutional operations, including governance actions and high-value transactions. ECDSA on secp256k1 is the dedicated layer for general-purpose transactions, with spend limits enforced by the protocol. The two layers have complementary roles; they do not carry identical permissions or identical security properties. Candidate primitives for the post-quantum layer include the signature schemes standardised by NIST in FIPS 204 and FIPS 205 (NIST, 2024b, 2024c) and schemes recognised by CyberSecurity Malaysia, with key encapsulation under FIPS 203 (NIST, 2024a) as an extension path. Adoption of each primitive remains subject to the applicable evaluation, certification and governance requirements.

**Independent validation as the assurance gate.** Formal validation, including CyberSecurity Malaysia evaluation under MySEAL where applicable, is the assurance gate for any primitive's approved production use. It enables institutions to assess the specific algorithm version, parameters and implementation against recognised requirements before relying on it for designated high-security operations. WalletSymLink preserves continuity for ECDSA transactions permitted by active protocol policies while validation proceeds, separating algorithm assurance from network continuity. Operational continuity does not waive certification requirements or authorise an ECDSA alias to perform actions reserved for the post-quantum layer.

**WalletSymLink: dual identity for agility and defence in depth.** Each participant holds a primary post-quantum address and may register an EVM alias address (20 bytes, secp256k1) through an on-chain WalletSymLink struct. The primary address anchors the participant's institutional signing identity; the EVM alias provides access for general-purpose transactions within protocol-enforced value thresholds. Existing EVM wallets, including MetaMask, operate through the alias, with address mappings resolved transparently by the protocol. High-value transactions and

governance actions require post-quantum signatures and cannot be authorised through the ECDSA alias. The Gemilang VM, a fork of the Ethereum Virtual Machine, handles address resolution; for post-quantum signature verification, `pqcrecover()` replaces `ecrecover()`, and other contract logic remains unchanged. The model is designed so that the underlying post-quantum primitive can be substituted through governance without changing a participant's on-chain identity or holdings.

**Long-duration assets and records.** For an asset or record created on-chain at time  $t$  with intended duration  $D$ , the security strategy must address the full interval  $[t, t + D]$ . ECDSA's security depends on the elliptic-curve discrete logarithm problem, which a sufficiently capable fault-tolerant quantum computer could solve using Shor's algorithm. Protocol spend limits bound the authority of the ECDSA alias; they do not make ECDSA quantum-resistant. The security of operations assigned to the post-quantum layer must in turn be assessed against the exact algorithm version, parameters, implementation and independent cryptanalytic evidence. MerdekaL1's long-term resilience therefore rests on three things together: validated primitives, risk-appropriate signing policies and the governed ability to replace cryptography as evidence changes.

**Alignment with Malaysia's national PQC readiness direction.** NACSA's National PQC Readiness Roadmap initiates PQC migration across NCII sectors and establishes a strategic framework for cryptographic governance, research and application (NACSA, 2025), and CyberSecurity Malaysia has published initiatives on migration guidance, cryptographic agility and quantum-safe adoption (CyberSecurity Malaysia, 2025). MerdekaL1 responds through a hybrid architecture that prioritises high-value institutional workflows and retains the ability to adopt recognised primitives as national and international guidance matures. Its security strategy is designed to evolve with NIST and CyberSecurity Malaysia guidance and the requirements of institutions operating in or adjacent to NCII sectors.

**Governed substitution as a resilience capability.** Cryptographic agility encompasses the algorithms, keys and signing primitives that establish transaction authority. The governance layer is designed to coordinate their replacement without network disruption, chain restarts or asset migration: migrating eligible transaction signing from ECDSA to the post-quantum layer, and substituting one approved post-quantum primitive for another as quantum threats, cryptanalytic evidence and institutional requirements evolve. Protocol policies determine which signing path may authorise each operation.

## // 2.2 MERDEKA CONSENSUS AND SETTLEMENT FINALITY

MerdekaL1 uses MERDEKA, Malaysian Enterprise Resilient Distributed Execution with Knowledge Authority, as its consensus foundation. MERDEKA is a Byzantine Fault Tolerant consensus engine written entirely in Go and purpose-built for institutionally governed blockchain infrastructure (MERDEKA, 2026). The engine implements proven BFT algorithms for distributed agreement among validators while separating technical consensus execution from institutional decision-making.

MERDEKA is designed to deliver deterministic settlement finality. The engine targets a planned validator set of 20 to 30 institutional participants drawn from across the financial, cybersecurity, regulated industry and government domains, and tolerates Byzantine faults in up to  $f = L(n-1)/3$  validators. Specific performance targets, including transactions per second and block time, are set out in the technical appendix and will be validated through testnet measurement before final mainnet claims are published.

This design aligns with Principle 8 of the Principles for Financial Market Infrastructures, which requires clear and certain final settlement (CPMI-IOSCO, 2012). Settlement finality is critical for financial system stability because it provides a baseline of clarity regarding the rights and relationships between parties (Cheng, 2020). Once a block is committed by more than two-thirds of the validator set through the multi-round voting protocol, the transaction is final. There is no probabilistic phase, no economic finality with reorganisation risk and no inheritance of finality risk from a base layer.

## // 2.3 GOVERNED EXECUTION ENVIRONMENT

The third architectural pillar makes MerdekaL1 useful for institutional workflows rather than only useful as cryptographic infrastructure. The execution environment is EVM-compatible, giving developers, auditors, custodians, public-sector bodies and solution providers a familiar developer surface, tooling and security practice. MerdekaL1 pairs this surface with native protocol-level controls, so that applications inherit institutional requirements from the protocol rather than reconstructing them at the application layer. Three controls are central.

**Identity-linked participation.** Participants interact with the network according to the level of verification a workflow requires, from individual and corporate verification to institutional credentials and regulated operator roles. A participant holds a wallet, but eligibility for specific

workflows depends on credential status, which is referenced, refreshed and revoked through defined procedures rather than enforced manually by each application. This avoids unnecessary exposure of personal or commercial data on-chain. Engagement with MyDigital ID is underway to explore integration as part of the identity-linked verification layer.

**Programmable compliance.** Regulatory, operator and workflow rules can be expressed as transaction-level controls, including transfer restrictions, eligibility checks, transaction limits and workflow-specific approvals. Where a workflow requires it, eligibility is checked before a transaction executes, and auditable records are preserved for operators, auditors and authorised observers. Applications inherit a common set of standardised controls and adapt them to their own requirements, rather than each implementing separate compliance logic in isolated smart contracts.

**Private permissioned access.** Transaction information is disclosed according to role, purpose and authority: neither full public exposure nor blanket anonymity. The model operates across four visibility tiers. The public integrity layer exposes network-level data such as block headers, transaction hashes, timestamps and aggregate activity to support auditability. Counterparty visibility gives the parties to a transaction the details required to verify their own records. Operator and auditor visibility gives custodians, operators and auditors information within the scope of their role or mandate. Regulator observer visibility gives authorised supervisory observers access to relevant records through defined procedures, access controls and audit logs. At the implementation level, the model combines role-based access control, credential-gated disclosure, encrypted data references, field-level permissioning and auditable access logs.

MerdekaL1 therefore combines permissioned, institutionally governed validation with an open, standard EVM developer surface: participation in consensus is governed, while building on the network uses the tools developers already know.

### **3 / GOVERNANCE OF QUANTUM-READY DIGITAL INFRASTRUCTURE**

#### **// 3.1 THE GOVERNANCE IMPERATIVE AND INTERNATIONAL GROUNDING**

For national digital infrastructure, achieving quantum readiness is fundamentally a strategic governance challenge. The objective extends beyond selecting cryptographic standards; it requires clear authority to govern their adoption, evolution, replacement and enforcement across systems that underpin national economic activity. Unlike previous technology upgrades, the quantum transition is a continuous process rather than a singular implementation exercise. Cryptographic standards will continue to evolve, new vulnerabilities may emerge and alternative algorithms may be standardised. A system capable of deploying a post-quantum algorithm must also possess the framework to govern its eventual replacement to remain quantum-ready. Without this adaptability, even robust cryptography operates within an institutionally rigid environment.

International approaches increasingly reflect this reality. The United States has separated standards determination from implementation governance through the roles of NIST and sector-specific regulators. The European Union has embedded cryptographic resilience within broader operational governance through the Digital Operational Resilience Act (European Parliament and Council, 2022). Singapore's Project Ubin demonstrated the value of regulatory experimentation and industry coordination before formal mandates are imposed, while Project Dunbar, Project Nexus and related initiatives led by the Bank for International Settlements highlighted the importance of governance alignment for cross-border interoperability (BIS Innovation Hub, 2022, 2023). These developments point toward a common conclusion: the critical enabler for quantum readiness is not merely the availability of technical solutions, but the institutional architecture required to make migration coordinated, accountable, auditable and durable.

#### **// 3.2 THE MERDEKA GOVERNANCE FRAMEWORK**

The MERDEKA Governance Framework is designed as a reusable governance architecture for national digital infrastructure. Rather than being tied to a specific sector or application, it provides a common governance foundation that can be applied across multiple domains of national significance. It separates standards determination, governance decision-making, regulatory execution and infrastructure deployment into distinct but interconnected layers. This separation reflects international practice and reduces the concentration of authority within any single institution.

At the standards layer, recognised authorities establish cryptographic, certification and cybersecurity requirements, which provide the technical foundation on which the infrastructure is built. At the governance layer, the MERDEKA Security Council provides multi-authority oversight for decisions with systemic consequences, including participant admission, protocol upgrades, cryptographic transitions, emergency response and governance of economic parameters. At the domain layer, existing statutory authorities continue to exercise their respective mandates: financial regulators govern financial infrastructure, cybersecurity agencies govern national cyber resilience, and digital economy and sectoral authorities govern the platforms within their remit. The framework coordinates existing authority rather than replacing it. At the infrastructure layer, the model is designed to apply first to financial infrastructure, and potentially to digital identity, public services, trade infrastructure and future national platforms.

The central proposition of the framework is that national digital infrastructure should be governed once and reused many times. Systems may differ in function, but they share common governance requirements relating to trust, accountability, resilience and cryptographic integrity.

### **// 3.3 THE MERDEKA SECURITY COUNCIL AS IMPLEMENTATION**

The MERDEKA Security Council is the institutional governance body designed to oversee the network. It is a planned 12-member round table comprising five permanent members representing core national interests across financial regulation, cybersecurity and other core national stakeholders, and seven rotating members representing broader stakeholder participation across financial institutions, regulated industry sectors, technology partners and academic and research bodies (MERDEKA, 2026). Final composition is subject to the network's launch governance process.

The Security Council's permanent members hold structural veto authority over protocol upgrades. This authority is a safety mechanism designed to prevent rushed or insufficiently scrutinised changes to systemic infrastructure rather than a unilateral block. Veto decisions are subject to a 30-day review period, must be accompanied by a public written justification entered onto the on-chain governance record and can be overridden by a 10/12 supermajority of the full Council. Validator admission and removal requires a 7/12 majority of the full Council. Emergency action requires three of five permanent member signatures and expires automatically after 48 hours unless ratified by the full Council. All proposals, votes and vetoes are recorded on-chain with cryptographic signatures.

The first principle, separation of standards authority from implementation governance, is satisfied by grounding cryptographic selection in external standards and validation, including NIST standards and CyberSecurity Malaysia's MySEAL framework. External standards and validation determine the assurance requirements for the selected primitives. The Security Council governs implementation timelines, transition provisions and deprecation conditions within that framework, including how changes apply to the distinct post-quantum and ECDSA roles. It does not determine the standards themselves or substitute governance approval for cryptographic validation.

The second principle, cryptographic agility as a governance hard requirement, is implemented through an upgrade procedure designed to substitute algorithms, keys and signing primitives without network disruption, chain restarts or asset migration. This provides a governed path from ECDSA to post-quantum signing, and between post-quantum primitives, as quantum threats, cryptanalytic evidence and recognised standards evolve. The Council coordinates adoption and deprecation within the externally defined assurance requirements, preserving the transaction permissions and institutional accountability of the hybrid model.

The third principle, multi-authority quorum for decisions with systemic consequences, is satisfied by the 12-member Council structure, with five permanent members spanning financial and cybersecurity governance and seven rotating members spanning financial institutions, regulated industry, technology and academic and research bodies.

The fourth principle, time-bounded emergency authority with mandatory ratification, is satisfied by the 48-hour expiry of emergency action absent full Council ratification.

The fifth principle, governed economic parameters, is satisfied by routing governance of the economic rules that determine how value moves across the system through the Security Council, which holds oversight of economic parameters alongside participant admission, protocol upgrades, cryptographic transitions and emergency response.

### **// 3.4 WHAT THIS MEANS FOR MALAYSIA**

Malaysia enters the post-quantum transition from a position of institutional strength. NACSA, CyberSecurity Malaysia and the MySEAL certification framework provide national cybersecurity authority and cryptographic certification capability, and Malaysia's financial regulators bring

established supervisory frameworks for financial market infrastructure. Few jurisdictions possess this combination of cybersecurity, certification and financial-supervisory capacity at the same time.

The strategic challenge therefore lies not in creating new institutions, but in designing governance arrangements that coordinate existing authorities while preserving their respective statutory mandates. In September 2026, e23 submitted a formal application to the NACSA/PTPKM Sandbox under the National PQC Migration Plan, which, if approved, would provide a structured setting in which to test the approach with the relevant authorities.

Three elements follow. The first is standards grounding: a credible quantum-ready governance model needs a technical standards reference that sits outside the network itself, which Malaysia has through CyberSecurity Malaysia, the MySEAL framework and NACSA's National PQC Readiness Roadmap (NACSA, 2025; CyberSecurity Malaysia, 2025). The second is regulatory sequencing: Singapore's approach offers a directly applicable precedent (Monetary Authority of Singapore, 2024), in which a phased path from awareness and inventory requirements, through sandbox-based learning, to binding expectations allows governance standards to be empirically grounded rather than theoretically derived. The third is regional design from the outset: post-quantum requirements for financial market infrastructure across ASEAN remain at an early stage, and infrastructure designed with regional interoperability as a founding constraint positions Malaysia to contribute meaningfully as regional approaches take shape.

Digital infrastructure of national significance derives legitimacy not from technical properties alone, but from the institutions that govern it. The detailed governance architecture will be documented in a forthcoming technical governance paper.

## 4 / USE CASE: INVOICE LIFECYCLE INFRASTRUCTURE

MerdekaL1's governance framework, consensus engine and hybrid security model are designed to support multiple applications. This paper presents one, invoice lifecycle infrastructure, as a concrete illustration of how the network can add a trusted verification layer to existing national digital systems without displacing them.

### // 4.1 THE OPPORTUNITY

Malaysia's e-invoicing mandate, administered by LHDN through MyInvois, operates under a Continuous Transaction Control model in which every commercial invoice is validated in real time and assigned a Unique Identifier Number before issuance to the buyer (Inland Revenue Board of Malaysia, 2026). This creates a nationally validated invoice record that did not previously exist, and an opportunity to address three structural gaps in invoice financing, a segment of particular importance to SMEs and part of the wider trade finance gap documented by the Asian Development Bank (Asian Development Bank, 2025).

The first gap is verification fragmentation: financiers rely on copies submitted by sellers without an independent means of verifying authenticity or validation status. The second is double-pledging risk: the same invoice can be pledged to multiple financiers without a shared record of existing claims. The third is reconciliation friction: lifecycle events, including issuance, validation, financing encumbrance, dispute flags and fulfilment confirmation, sit across disconnected systems.

### // 4.2 HOW MERDEKAL1 SUPPORTS IT

MerdekaL1 represents each MyInvois-validated e-invoice as a unique, non-fungible on-chain record carrying the invoice hash, validation status, parties, amount and Unique Identifier Number. The record is a verification and audit-trail layer on top of the existing MyInvois infrastructure, not a replacement for it.

Licensed financiers use this layer within their own authorised financing workflows. Banks and factoring companies can verify the authenticity and unencumbered status of an invoice before extending financing. Once financing is extended, the record is flagged to prevent double-pledging. Lifecycle events are captured for authorised parties under the four-tier visibility model described in Section 2.3, and the identity-linked participation and programmable compliance controls govern who may view, flag or release a record.

**// 4.3 POSITIONING AND NEXT STEPS**

The infrastructure does not tokenise invoices as tradeable securities and does not process payments. It is designed so that MerdekaL1 does not itself require a payment or financial services licence, subject to confirmation with the relevant authorities; licensed institutions continue to operate under their own authorisations. The use case is presented as a proof of concept. Its regulatory feasibility and integration requirements, including any interface with MyInvois, are to be validated with the relevant authorities before implementation, and it reflects the direction being worked toward rather than an established arrangement.

For the digital economy, the significance extends beyond invoice financing. The same pattern, a governed verification layer anchored to an authoritative government record, is reusable wherever trusted digital records underpin access to finance or public services.

## 5 / CURRENT PROGRESS AND ROADMAP

The MerdekaL1 roadmap is structured around progressive institutional readiness. The work has moved beyond concept definition into issuance demonstration, MVP build-out and early regulatory engagement.

| STATUS      | ITEM                         | TARGET        | NOTES                                                               |
|-------------|------------------------------|---------------|---------------------------------------------------------------------|
| Completed   | Token issuance workflow      | Q4 2025       | End-to-end issuance workflow demonstrated                           |
| Completed   | Core issuance capabilities   | Q1 2026       | Token creation and lifecycle in place                               |
| In Progress | L1 hybrid cryptography MVP   | TBD           | Core network + validator coordination                               |
| Engagement  | NACSA-PTPKM sandbox          | 2026          | Active application                                                  |
| Engagement  | National systems integration | TBD           | Broader ecosystem alignment                                         |
| Planned     | Mainnet beta                 | 2027 (target) | Subject to PQC primitive validation, audit and regulatory clearance |

The architectural commitments in this paper frame the next phase: cryptographic agility; complementary post-quantum and ECDSA signing roles; the WalletSymLink dual-identity model; MERDEKA BFT consensus; Security Council governance; and EVM-compatible execution through the Gemilang VM. Selection and validation of the production post-quantum primitive, independent audit and sandbox completion remain explicit launch and assurance gates, with signing permissions governed according to the approved production scope. Subsequent work covers expanded institutional validator participation, additional validated primitives and the evolution of privacy controls from gateway-based access toward zero-knowledge proof mechanisms for sensitive flows.

## 6 / WHAT e23 BRINGS TO THE TASKFORCE

MerdekaL1 is shared with the taskforce as a reference for what Malaysian-built, institutionally governed blockchain infrastructure can look like, and as a basis for practical collaboration. e23 can contribute in four areas.

**Domestic capability.** The core components of MerdekaL1, namely the MERDEKA consensus engine, the Gemilang VM and the MERDEKA Governance Framework, are designed and developed by e23 in Malaysia. This supports Malaysia's ambition to build, rather than import, the infrastructure on which critical digital services depend, and develops local expertise in consensus engineering, post-quantum migration and digital infrastructure governance.

**Ecosystem access.** Because MerdekaL1 is EVM-compatible, Malaysian developers, auditors and solution providers can build on it with existing tools, languages and security practices. This lowers the barrier for local firms to develop regulated applications and positions the developer community to take part in institutional and public-sector projects.

**Reference architecture and pilot design.** e23 can make available to the taskforce the MerdekaL1 reference architecture and governance framework, the MERDEKA consensus engine technical specification and technical briefings for participating agencies, together with a proposed design for a proof-of-concept pilot, such as the invoice verification use case in Section 4, scoped jointly with the relevant authorities and institutions.

**Institutional and standards participation.** e23 welcomes engagement from licensed institutions, government-linked entities, academic and research bodies and cryptographic standards bodies on validator participation, Security Council design and the validation of post-quantum primitives.

## 7 / CONCLUSION

The next generation of digital infrastructure must be programmable, governable, interoperable and quantum-ready. MerdekaL1 is built for that requirement from the ground up.

Cryptographic agility leads its hybrid architecture. The governance layer is designed to substitute algorithms, keys and signing primitives without network disruption, chain restarts or asset migration, so that no single primitive becomes a single point of failure. The MERDEKA consensus engine provides deterministic finality, the MERDEKA Security Council provides multi-authority governance that coordinates rather than replaces existing statutory mandates, and the Gemilang VM provides familiar EVM execution with protocol-level controls for identity, compliance and privacy.

The work is under way. Core issuance capabilities have been demonstrated, the L1 hybrid cryptography MVP is in active development and e23 is participating in the NACSA and PTPKM regulatory sandbox. e23 welcomes the opportunity to work with MDEC and the taskforce on how this infrastructure can support Malaysia's digital economy. Engagement enquiries are welcomed at [contact@e23.io](mailto:contact@e23.io).

## REFERENCES

1. Asian Development Bank (2025) ADB Global Trade Finance Gap Survey. Manila: Asian Development Bank. Available at: <https://www.adb.org/publications/adb-global-trade-finance-gap-survey> (Accessed: April 2026).
2. BIS Innovation Hub (2022) *Project Dunbar: international settlements using multi-CBDC*. Basel: Bank for International Settlements. Available at: <https://www.bis.org/publ/othp47.htm>.
3. BIS Innovation Hub (2023) *Project Nexus: enabling instant cross-border payments*. Basel: Bank for International Settlements. Available at: <https://www.bis.org/about/bisih/topics/fmis/nexus.htm>.
4. Cheng, J. (2020) 'How to build a stablecoin: certainty, finality, and stability through commercial law principles', *Berkeley Business Law Journal*, 17(2).
5. CPMI-IOSCO (2012) *Principles for financial market infrastructures*. Basel: Bank for International Settlements. Available at: <https://www.bis.org/cpmi/publ/d101.htm>.
6. CyberSecurity Malaysia (2025) *Post-Quantum Cryptography migration guidance and the MySEAL framework*. Available at: <https://mykripto.cybersecurity.my/index.php/services/post-quantum-cryptography-initiatives/documents> (Accessed: April 2026).
7. European Parliament and Council (2022) *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)*. Brussels: Official Journal of the European Union.
8. G7 Cyber Expert Group (2026) *Statement on advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector*. Available at: <https://assets.publishing.service.gov.uk/media/6966149d8d599f4c09e1ffab/G7-CEG-Quantum-Roadmap.pdf>
9. Google Quantum AI (2026) *Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly*. Available at: <https://research.google/blog/safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly/> (Accessed April 2026).
10. Inland Revenue Board of Malaysia (2026) *e-Invoice Guideline (Version 4.6)*. Kuala Lumpur: Lembaga Hasil Dalam Negeri Malaysia. Available at: <https://www.hasil.gov.my/en/e-invoice/> (Accessed: April 2026).
11. MERDEKA (2026) *Consensus Engine Technical Specification v1.0: a Byzantine Fault Tolerant consensus engine with institutional governance*. January 2026.
12. Monetary Authority of Singapore (2024) *Advisory on addressing the cybersecurity risks associated with quantum*. Available at: <https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum>
13. NACSA (2025) *National PQC Readiness Roadmap*. Putrajaya: National Cyber Security Agency Malaysia. Available at: <https://mykripto.cybersecurity.my/index.php/files/109/Post-Quantum/18/Post-quantum-Cryptography-Migration-Framework.pdf> (Accessed April 2026).
14. NIST (2024a) *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://csrc.nist.gov/pubs/fips/203/final>
15. NIST (2024b) *FIPS 204: Module-Lattice-Based Digital Signature Standard*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf>
16. NIST (2024c) *FIPS 205: Stateless Hash-Based Digital Signature Standard*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: <https://csrc.nist.gov/pubs/fips/205/final>

17. Securities Commission Malaysia (2026) *Capital Market Masterplan 2026–2030*. Kuala Lumpur: Securities Commission Malaysia. Available at: <https://www.sc.com.my/capital-market-masterplan> (Accessed April 2026).
18. Shor, P. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press.

## TECHNICAL APPENDIX: PERFORMANCE DESIGN TARGETS

Design targets based on MERDEKA consensus architecture parameters: approximately 5,000 transactions per second at the consensus layer, sub-2-second block time, deterministic Byzantine Fault Tolerant finality, and signature verification at approximately 2,000 signatures per second per core under post-quantum signature scheme hardware acceleration profiles.

These figures are architectural design targets and will be replaced with measured testnet benchmarks prior to mainnet publication. Measured benchmarks will be published alongside the L1 hybrid cryptography MVP testnet release.

## DISCLAIMER

This litepaper is for general information purposes only. It does not constitute investment advice, legal advice, tax advice, accounting advice, or a recommendation or solicitation to buy or sell any security, token or financial instrument. It should not be relied upon for the evaluation of the merits of any investment decision. MerdekaL1 is offered by e23 Sdn Bhd. The legal entity is a software and infrastructure provider and does not provide regulated financial or advisory services. All product features described herein may be modified, delayed or cancelled without prior notice at the sole discretion of the issuing entity. Persons engaging with e23 services are solely responsible for obtaining any necessary licences or approvals and otherwise complying with applicable laws in their jurisdiction. References to NIST standards, the MySEAL framework, NACSA's National PQC Readiness Roadmap, CyberSecurity Malaysia, the Capital Market Masterplan 2026–2030, LHDN's MyInvois system and the NACSA and PTPKM regulatory sandbox are provided for context only and do not constitute regulatory endorsement of e23. The governance arrangements described in this litepaper, including the composition, powers and voting thresholds of the MERDEKA Security Council, are proposals by e23 and are subject to the network's launch governance process. They do not indicate that any authority, agency or institution referred to has agreed to participate in, or has approved, those arrangements.

This litepaper contains forward-looking statements, including statements on development timelines, performance targets, the selection and validation of cryptographic primitives and regulatory engagement. These statements reflect e23's current intentions and are subject to technical validation, independent audit, regulatory and commercial factors, many of which are outside e23's control. Actual outcomes may differ materially. This litepaper is provided in confidence for the purpose of evaluation by the recipient and may not be reproduced or distributed further without e23's prior written consent. Performance figures cited from the MERDEKA technical specification are design targets to be validated through testnet measurement before final mainnet claims are published.

© 2026 e23. All rights reserved.