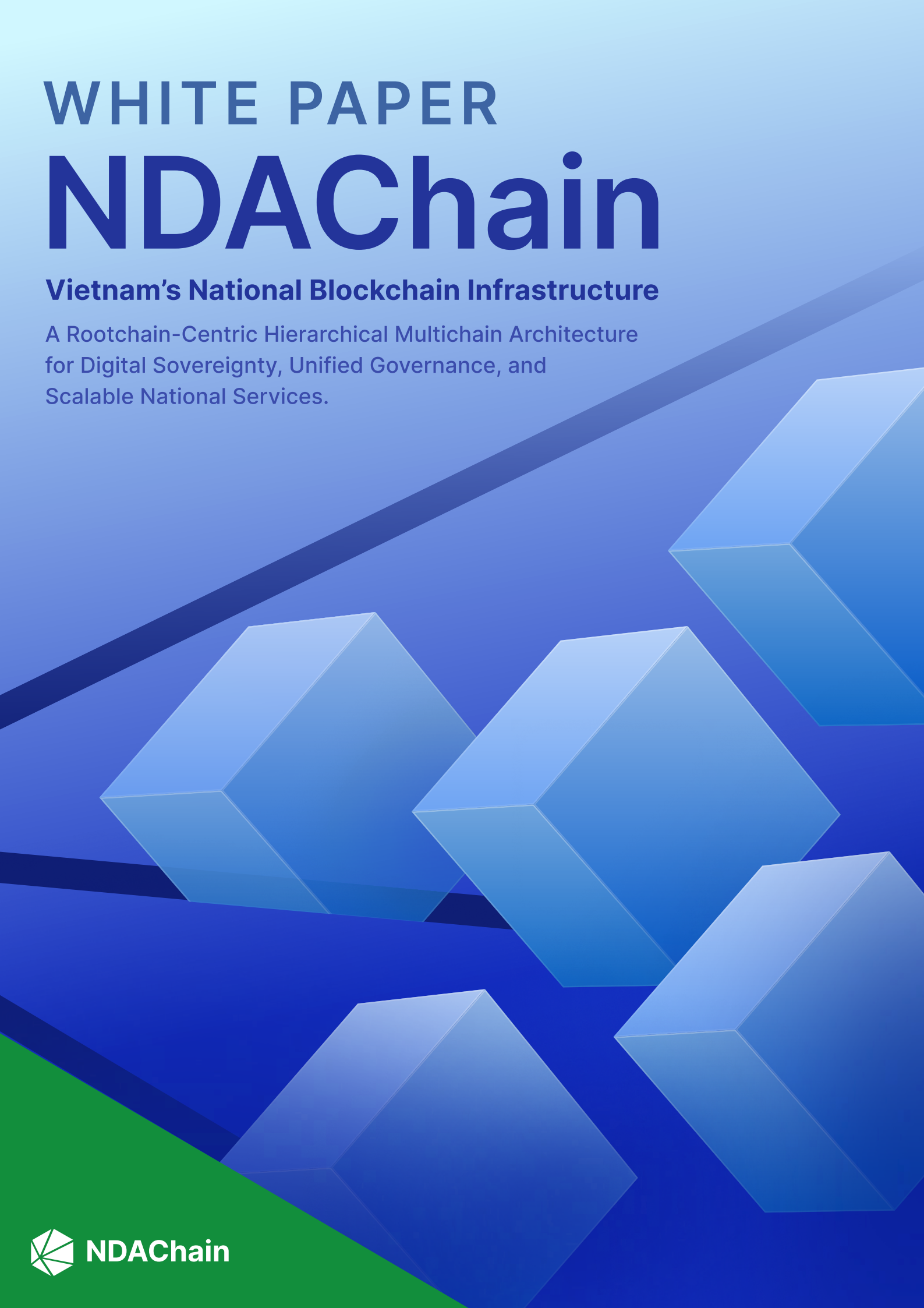
WHITE PAPER

NDAChain

Vietnam's National Blockchain Infrastructure

A Rootchain-Centric Hierarchical Multichain Architecture for Digital Sovereignty, Unified Governance, and Scalable National Services.



NDAChain

NDAChain: Vietnam's National Blockchain Infrastructure

A Rootchain-Centric Hierarchical Multichain Architecture
for Digital Sovereignty, Unified Governance, and Scalable National Services

Executive Summary

NDAChain is Vietnam's sovereign national blockchain infrastructure, designed to deliver digital sovereignty, unified governance, and high-performance services across the nation. Built as a rootchain-centric hierarchical multichain architecture, NDAChain addresses the unique requirements of a mid-sized unitary state by combining strong centralized oversight with flexible, sector-specific scalability.

At its core, NDAChain features a permissioned Rootchain (NDAChain Trust Layer) that serves as the single source of truth and control tower for the entire ecosystem. This Rootchain anchors decentralized identities (DID) for all participating entities and enforces national policy through a robust governance framework, including Special Administrative Keys (threshold multi-signature) for rapid yet auditable emergency intervention. Specialized Domain Chains connect to the Rootchain, enabling both horizontal scaling (adding new chains for different sectors) and vertical scaling (independent performance optimization within each chain). This design directly implements the rootchain-centric model proposed in the accompanying academic paper, transforming theoretical advantages into a production-ready national platform.

A key innovation is ChainHub, the identity-driven interoperability layer built on the Chain-as-Entity Identity mechanism. Each Domain Chain is treated as a first-class identity subject with its own Decentralized Identifier (DID) and granular Verifiable Credentials (VC). This enables a dual-gate runtime authorization engine that combines cryptographic state proofs with identity-based permission checks. Domain Chains can interact directly using Verifiable Presentations (VP) without routing every transaction through the Rootchain, reducing central load while maintaining full national traceability and real-time revocation. The architecture is technology-agnostic, allowing existing blockchains (EVM-based, permissioned enterprise blockchains, custom chains, and Layer 2) to integrate without core modifications.

NDAChain incorporates a sovereign decentralized storage layer — NDA Secure File System (NDA SFS) — with multi-tier (local → regional → national) nodes, end-to-end encryption, and identity-centric access control. All critical operations benefit from gas-free or near-zero-cost execution for public services, aligning with national digital transformation goals.

Real-world evaluation on prototypes, national testnet, and early production deployments demonstrates strong performance: the Rootchain sustains approximately 1,200 Write TPS with deterministic finality under 2.5 seconds, while the ecosystem achieves an aggregate throughput exceeding 100,000 TPS across multiple Domain Chains. The system maintains ≥99.95% uptime with validators distributed across three geographic regions (North, Central, South), delivering predictable low-latency governance and cross-chain operations suitable for nationwide services.

NDAChain strikes a practical balance between decentralization and state oversight that is particularly well-suited to Vietnam's scale and unitary governance model. Compared to large-scale federated systems such as China's BSN or the EU's EBSI, it offers superior unified control, immediate auditability, simpler governance, and faster emergency response with fewer attack surfaces.

By anchoring national digital identity, secure data sharing, supply chain traceability, and e-governance services on a single sovereign infrastructure, NDAChain provides the foundational layer for Vietnam's digital economy. It realizes the strategic vision of Decision 1236/QĐ-TTg (2024) while establishing a scalable, secure, and controllable blockchain foundation for the nation's long-term digital sovereignty.

Table of contents

1. Introduction

Vietnam is advancing rapidly toward its digital transformation goals, aiming to build a secure, sovereign, and scalable digital infrastructure that serves both public services and economic development. With a population of approximately 100 million and a unitary governance structure, the country requires a national blockchain platform that ensures digital sovereignty, unified state oversight, regulatory compliance, data residency, and high scalability across multiple sectors.

The National Blockchain Strategy (Decision 1236/QĐ-TTg, 2024) underscores these priorities, calling for a national infrastructure that supports traceability, secure data sharing, and sector-specific applications while maintaining strong governmental control. A purely centralized single-chain system would face severe performance and flexibility limitations, while highly decentralized or federated models risk fragmenting authority and complicating national-level auditability and policy enforcement.

To meet these requirements, NDAChain has been designed as a rootchain-centric hierarchical multichain architecture. At its foundation is a permissioned Rootchain (NDAChain Trust Layer) that acts as the central control tower and single source of truth for the entire national ecosystem. Multiple specialized Domain Chains connect to this Rootchain, inheriting identity, trust, and governance policies while retaining independence in consensus mechanisms, performance optimization, and sector-specific business logic.

This hierarchical approach enables both horizontal scaling — by adding new Domain Chains for different national sectors such as digital identity, supply chain traceability, healthcare records, education credentials, financial services, and e-governance — and vertical scaling — by independently tuning performance and capacity within each Domain Chain. The Rootchain manages critical functions including whitelist approval of participating chains, identity anchoring through Decentralized Identifiers (DID), issuance and lifecycle management of Verifiable Credentials (VC), cross-chain authorization, and verifiable proof-of-control for all inter-chain activities.

A distinctive feature of NDAChain is its Chain-as-Entity Identity model, in which each Domain Chain is treated as a first-class identity subject. This enables a dual-gate runtime authorization mechanism that combines cryptographic state proof verification with identity-based permission checks. Domain Chains can interact directly with one another using Verifiable Presentations (VP), reducing load on the Rootchain while preserving complete national-level traceability and real-time revocation capabilities.

NDAChain is further supported by the NDA Secure File System (NDA SFS), a sovereign multi-tier decentralized storage layer that ensures end-to-end encrypted, identity-centric data sharing in full compliance with Vietnam's personal data protection and data residency regulations.

This whitepaper provides a comprehensive description of the NDAChain architecture, its technical design, governance mechanisms, security features, and real-world performance. It outlines how NDAChain delivers a practical balance between strong centralized oversight and scalable, sector-specific execution, making it particularly well-suited to Vietnam's national context and strategic objectives.

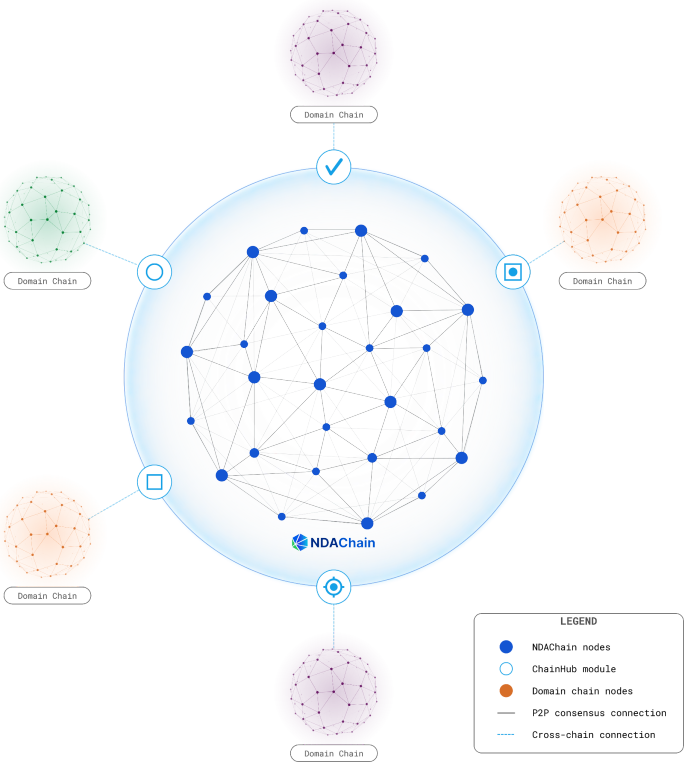
The remainder of this whitepaper is organized as follows: Section 2 discusses the design rationale and national context; Section 3 presents the high-level architecture; Section 4 details the Rootchain; Section 5 explains the ChainHub; Sections 6–9 cover Domain Chains, sovereign storage, security, and governance; Section 10 presents implementation status and performance results; and Section 11 provides comparative analysis and strategic advantages.

2. Design Rationale and National Context

Vietnam's digital economy is growing rapidly, driven by strong government commitment to digital transformation, e-government services, and secure data infrastructure. To support this ambition, the National Blockchain Strategy (Decision 1236/QĐ-TTg, 2024) sets clear objectives: establishing digital sovereignty, ensuring data residency within national borders, enabling unified governance and traceability, and delivering scalable blockchain services for both public and private sectors.

These goals create a distinct set of requirements that differ from those of much larger economies or multi-sovereign unions. Vietnam needs a blockchain infrastructure that provides strong centralized policy enforcement and national-level auditability while still supporting high-throughput, sector-specific applications. A single monolithic blockchain would quickly encounter performance bottlenecks and struggle to accommodate diverse use cases such as digital identity, supply chain traceability, healthcare records, education credentials, and e-governance. At the same time, fully decentralized or loosely federated models risk fragmenting control, weakening traceability, and complicating regulatory compliance.

Figure 1: Overview of Vietnam Blockchain Ecosystem



2.1 Challenges of Existing National Blockchain Approaches

International experiences highlight important trade-offs in national blockchain design:

- China's Blockchain-based Service Network (BSN) adopts a federated "network of networks" model. It achieves massive scale through standardization and policy coordination but offers limited technical-level centralized traceability and unified governance across participating chains.
- European Union's European Blockchain Services Infrastructure (EBSI) uses a peer-to-peer permissioned network across member states. It prioritizes cross-border interoperability and self-sovereign identity while deliberately avoiding any central technical root to respect national sovereignty. This results in complex coordination and reduced real-time auditability.
- India's National Blockchain Framework (Vishvasya) provides a distributed Blockchain-as-a-Service model focused on public services. While centrally governed at the policy level, it lacks a single authoritative control layer for consistent cross-chain oversight.

These architectures are well-suited to their respective contexts — very large scale (China and India) or multi-sovereign coordination (EU). However, they are less optimal for a mid-sized unitary state like Vietnam, where the total number of participating chains is expected to remain manageable (tens to low hundreds initially), and strong national oversight is a strategic priority.

2.2 Requirements Specific to Vietnam

Based on the National Blockchain Strategy and broader national digital architecture frameworks (Decision 3090/QĐ-BKHCN and Decision 2439/QĐ-TTg), NDAChain must satisfy the following core requirements:

Strategic and Governance Requirements

- Full digital sovereignty and data residency within Vietnam's territory.
- Unified state control with clear accountability and immediate auditability of all critical operations.
- Strong support for KYC/AML/CFT, personal data protection law 2023, and electronic transaction legality.
- Efficient policy enforcement and emergency response capabilities at the national level.

Technical and Operational Requirements

- High scalability through both horizontal (adding new Domain Chains) and vertical (increasing capacity per chain) mechanisms.
- Differentiated performance: reliable control-plane operations on the Rootchain and high-throughput execution on Domain Chains.
- Secure and controlled cross-chain interoperability without compromising oversight.
- Security-by-design and privacy-by-design principles, including end-to-end encryption, Zero-Knowledge Proofs, and real-time revocation.
- High availability (target ≥ 99.95% uptime) and resilience against partial failures.
- Gas-free or near-zero cost operations for public services to drive widespread adoption.

2.3 The Rootchain-Centric Hierarchical Multichain Approach

NDAChain addresses these requirements through a rootchain-centric hierarchical multichain architecture. The permissioned Rootchain serves as the central trust anchor and governance layer. All Domain Chains must register their identity on the Rootchain and receive capability credentials before participating in the ecosystem. This creates a single source of truth for identity, authorization, and auditability while allowing Domain Chains to operate independently for sector-specific workloads.

This design delivers several key advantages for Vietnam:

- Unified Oversight: The Rootchain provides whitelist management, periodic audits, cross-chain traceability, and verifiable proof-of-control in one authoritative layer.
- Balanced Scalability: Control-plane operations (governance, identity, authorization) remain predictable and stable on the Rootchain, while execution-plane workloads scale independently across Domain Chains.
- Efficient Governance: Changes to chain permissions, roles, or access rights can be executed dynamically with immediate effect across the ecosystem.
- Reduced Complexity: With a moderate expected number of Domain Chains, a single well-protected Rootchain is more practical and secure than managing hundreds of fully independent nodes or complex peer-to-peer coordination.

The architecture also incorporates a sovereign decentralized storage layer (NDA SFS) with multi-tier nodes (local, regional, national) and strict identity-based access control. This ensures data remains within national boundaries while enabling secure, owner-controlled sharing across government agencies, enterprises, and citizens.

2.4 Alignment with National Digital Strategy

NDAChain is fully aligned with Vietnam’s broader digital architecture, including the four-layer national digital framework and requirements for interoperability, security level 4, and data sovereignty. It supports seamless integration with national platforms such as the Public Service Portal, VNeID, and other critical digital systems.

By combining strong centralized control at the Rootchain with flexible, specialized execution on Domain Chains, NDAChain provides a pragmatic and future-proof foundation. It avoids the extremes of full centralization (performance limitations) and full decentralization (loss of control), delivering an optimal balance for Vietnam’s scale, governance model, and strategic priorities.

3. NDAChain High-Level Architecture

NDAChain is designed as a rootchain-centric hierarchical multichain architecture that balances strong national control with flexible scalability. The system organizes the entire national blockchain infrastructure into four logical layers, ensuring clear separation of responsibilities while maintaining unified governance and trust.

3.1 Four-Layer Architecture

NDAChain consists of the following layers:

1. **Infrastructure Layer** The foundational physical and network layer, including servers, data centers, networking equipment, and security systems distributed across Vietnam. This layer provides the hardware and connectivity required for high availability and resilience. Nodes are geographically distributed across three regions (North, Central, and South) to ensure redundancy and low-latency access.

2. **Trusted Platform Layer (NDAChain Rootchain)** The core permissioned blockchain that serves as the central trust anchor and control tower for the entire ecosystem. This layer is responsible for national-level identity management, governance, authorization, and cross-chain oversight. All critical decisions and audit records are anchored here, making it the single source of truth.
3. **Domain & Execution Layer** This layer consists of multiple specialized Domain Chains (sector-specific permissioned blockchains) that handle actual business logic and high-volume transactions. Each Domain Chain operates independently but is integrated through ChainHub, inherits identity, trust, and permissions from the Rootchain. This separation allows high throughput for sector-specific workloads without overloading the control layer.
4. **Application Layer** The top layer where end-user applications, government services, enterprise systems, and citizen-facing dApps interact with the infrastructure. This layer includes core NDA applications (such as NDA Key wallet, NDA Trace, and NDA Drive) as well as ecosystem applications developed by ministries, provinces, and private partners.

3.2 Core Components and Their Roles

- **NDAChain Rootchain (Trust and Control Layer)** The Rootchain is implemented as a permissioned blockchain using Proof-of-Authority (PoA) consensus with QBFT for low latency and deterministic finality. It hosts the Decentralized Identifier (DID) Registry, manages Verifiable Credentials (VC) for chains and entities, and runs the Runtime Authorization Engine. All Domain Chains must register on the Rootchain and receive capability credentials before participating in the ecosystem. The Rootchain also maintains an immutable audit log of critical cross-chain activities.
- **Domain Chains (Sector-Specific Execution Layer)** Domain Chains are independent permissioned blockchains optimized for particular national sectors or use cases, such as supply chain traceability, healthcare records, education credentials, financial services, or e-governance. They can use different consensus parameters and performance configurations tailored to their workload. Each Domain Chain connects to the Rootchain with ChainHub, which allows it to securely verify identity and permission status.
- **NDA Secure File System (NDA SFS)** A sovereign, multi-tier decentralized storage system that complements the blockchain layers. Data is encrypted at the client side using keys tied to the data owner's DID, fragmented, and distributed across local, regional, and national storage nodes. Access is strictly controlled through Verifiable Credentials and Presentations, ensuring zero-trust storage — storage nodes never see plaintext data.
- **ChainHub (Interoperability and Authorization Framework)** ChainHub serves as the coordination and authorization layer for cross-chain interaction. While the Rootchain mediates governance and critical events, ChainHub enables efficient direct communication between Domain Chains through Verifiable Presentations (VP) and identity-based authorization. This hybrid model reduces load on the Rootchain while preserving full national traceability and real-time revocation.

3.3 Key Design Principles

The architecture follows several guiding principles derived from national requirements:

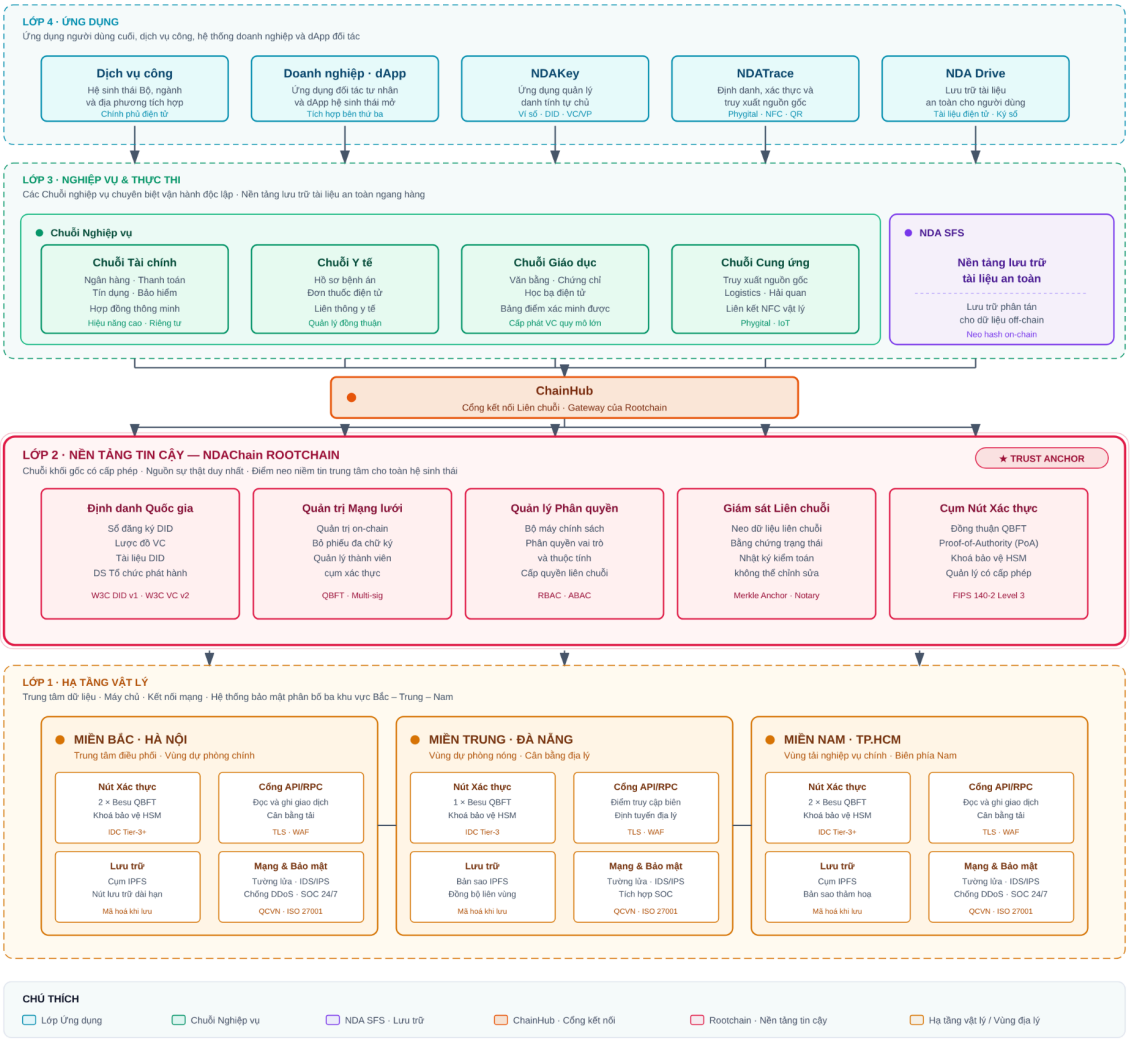
- Unified Control with Distributed Execution: Strong governance and identity anchoring remain centralized on the Rootchain, while execution workloads are distributed across Domain Chains.
- Technology-Agnostic Connectivity: Domain Chains can be built on different underlying technologies (EVM, other DLT frameworks, or custom implementations) as long as they integrate with the Rootchain's identity and authorization mechanisms.
- Identity-Centric Security: Every chain and major entity is assigned a Decentralized Identifier (DID). Permissions are managed through granular Verifiable Credentials (VC), enabling fine-grained, dynamic, and auditable access control.
- Gas-Free Public Services: The Rootchain operates with zero base fee for public-sector transactions to encourage broad adoption across government agencies and citizens.
- High Availability and Resilience: Validators are distributed geographically, with built-in fault tolerance and automated failover mechanisms targeting ≥ 99.95% uptime.

3.4 High-Level System Flow

When a Domain Chain needs to interact with another chain or submit critical state updates:

1. The sending chain presents its identity (DID) and capability credentials (via VP).
2. The receiving chain or Rootchain performs dual-gate validation: cryptographic proof + identity/permission check.
3. Approved interactions are processed, with critical events anchored back to the Rootchain for auditability.
4. All access to stored data in NDA SFS is similarly controlled through DID and VC/VP mechanisms.

Figure 2: High-level NDAChain Architecture



This layered, hierarchical design ensures that NDAChain can scale efficiently while maintaining the strong national oversight required for critical public infrastructure.

4. The Rootchain (NDAChain Core) – Trust and Governance Layer

The Rootchain is the heart of NDAChain and serves as the central trust anchor and governance layer for the entire national blockchain ecosystem. It is designed to provide unified control, identity management, authorization, and auditability while maintaining high reliability and predictable performance suitable for national-scale operations.

4.1 Role and Design Objectives

The Rootchain acts as the single source of truth for the national blockchain infrastructure. Its primary responsibilities include:

- Anchoring decentralized identities (DID) for all participating Domain Chains and major entities.
- Managing the issuance, update, and revocation of Verifiable Credentials (VC) that define permissions and roles.
- Enforcing runtime authorization for all cross-chain and critical operations.

- Maintaining an immutable audit log of governance actions and inter-chain activities.
- Providing verifiable proof-of-control for regulatory compliance and national oversight.

By concentrating these control-plane functions on one well-protected layer, the Rootchain enables strong national sovereignty while allowing Domain Chains to focus on high-volume sector-specific execution.

4.2 Technical Implementation

The Rootchain is implemented as a permissioned blockchain using Proof-of-Authority (PoA) consensus with the QBFT (Quorum Byzantine Fault Tolerance) protocol. This choice delivers deterministic finality, low latency, and energy efficiency while supporting the strict governance requirements of a national infrastructure.

Key Technical Specifications:

- Consensus Mechanism: QBFT (PoA variant) – tolerates up to 1/3 faulty or malicious validators.
- Block Time: 2.5 seconds (± 0.2 seconds).
- Finality: Deterministic finality under 2.5 seconds for critical operations.
- Write Throughput: Sustained ~1,200 transactions per second (TPS) under mixed governance and DID/VC issuance workloads (measured on production-grade testnet).
- Gas Policy: Zero base fee (zeroBaseFee = true) for public services, making the Rootchain effectively gas-free for government and citizen-facing applications.
- Virtual Machine: Ethereum Virtual Machine (EVM) compatible, supporting Solidity smart contracts.
- Deployment Environment: Production-grade infrastructure in national data centers with geographic redundancy (North, Central, South regions).

The Rootchain operates in a fully permissioned mode. Only pre-approved validators selected through a transparent national process may participate in block production.

4.3 Network Structure and Validator Model

The Rootchain network is distributed across Vietnam to ensure resilience and low latency:

- Validator Nodes: High-trust organizations including central ministries, major state-owned enterprises, and technology leaders. Validators are selected based on technical capability, legal standing, and strategic contribution.
- Operating Nodes: Additional full nodes run by approved enterprises and government agencies for data synchronization and querying (do not participate in consensus).
- Geographic Distribution: Validators are deployed in at least three regions (North – Hanoi area, Central – Da Nang, South – Ho Chi Minh City) to provide regional redundancy and fault tolerance.

Table 1: Rootchain Performance Targets (Measured on Testnet)

Metric	Target Value	Notes
Write TPS (governance & anchoring)	~1,200 TPS	Sustained under real mixed workloads
Finality	≤ 2.5 seconds	Deterministic
Block Time	2.5 seconds (± 0.2 s)	Configurable via genesis
Uptime	≥ 99.95%	Achieved in extended testnet runs
Fault Tolerance	Up to 1/3 validators	QBFT consensus

Metric	Target Value	Notes
Storage (per validator)	> 12 months / 1 TB	Efficient state pruning supported

4.4 Trustee Keys and Special Administrative Keys

Critical governance actions are protected by a **threshold multi-signature scheme** using **Trustee Keys** (also referred to as Special Administrative Keys). These keys are held by a small, carefully selected group of national trustees (typically 3–5 high-level entities).

- Threshold: m-of-n multi-signature (e.g., 2/3 or 3/5 approval required).
- Protected Operations: Protocol upgrades, validator addition/removal, emergency chain suspension, major policy changes.
- Auditability: All actions performed with Trustee Keys are mandatorily recorded on the Rootchain with full cryptographic proof, ensuring transparency even for emergency interventions.
- Security: Keys are stored in Hardware Security Modules (HSMs) with strict rotation and access policies.

This mechanism enables rapid response to security incidents or policy needs while preserving immutable audit trails — a crucial balance for national infrastructure.

4.5 Identity and Credential Management

The Rootchain hosts the DID Registry, which assigns and manages Decentralized Identifiers for every Domain Chain and major participating entity. Each Domain Chain is registered as a first-class identity subject, independent of its operators or users.

- DID Document: Contains public keys, endpoints, and metadata of the chain.
- Verifiable Credentials (VC): Issued by the Rootchain to define granular permissions (roles, allowed operations, rate limits, validity periods).
- Revocation: Real-time revocation of DIDs or VCs is supported through an on-chain revocation registry, with immediate effect on subsequent authorization checks.

4.6 Runtime Authorization Engine

All interactions involving the Rootchain or between Domain Chains (when anchored) pass through the Runtime Authorization Engine. This engine performs dual-gate validation:

1. Cryptographic Gate: Verification of signatures and state proofs.
2. Identity Gate: Resolution of DID and validation of associated VC (checking validity, revocation status, and permission scope).

Only requests that pass both gates are accepted. This design ensures strong security without creating performance bottlenecks for routine operations.

4.7 Governance and Upgrade Mechanisms

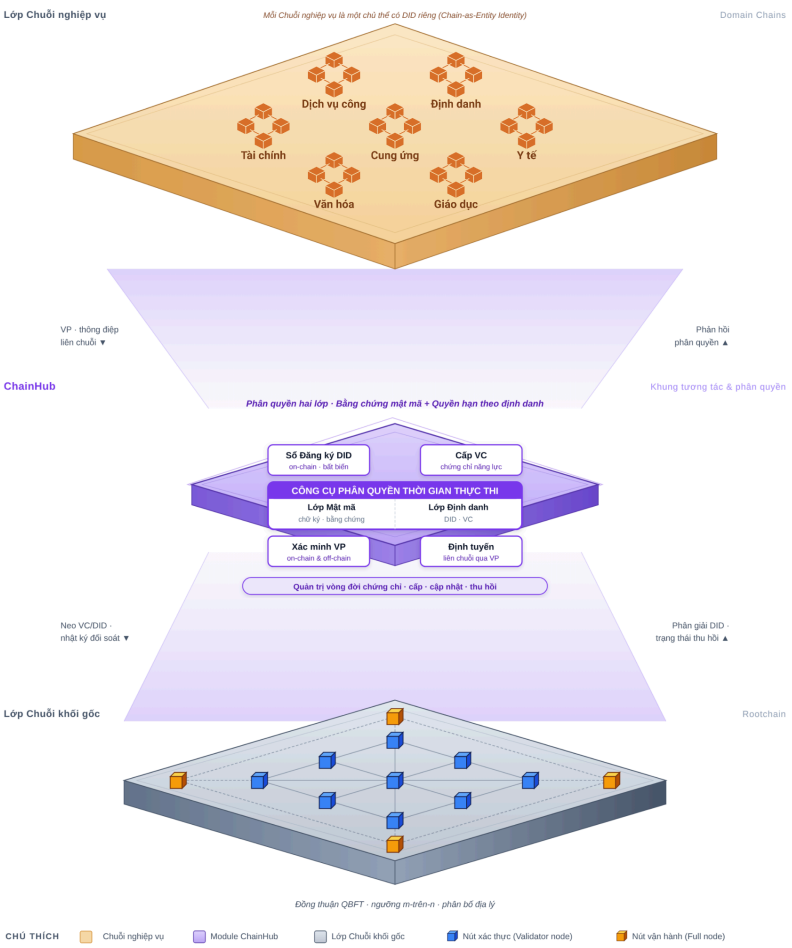
The Rootchain supports controlled upgrades through smart contract governance. Major changes require approval via Trustee Keys, while minor parameter adjustments can be executed through on-chain voting by validators. All upgrades are transparent and auditable.

This combination of technical robustness, geographic distribution, threshold governance, and identity-centric control makes the NDAChain Rootchain a secure, reliable, and sovereign foundation for Vietnam’s national blockchain ecosystem.

5. ChainHub - Identity and Interoperability Framework

A core innovation of NDAChain is its Chain-as-Entity Identity model, where each Domain Chain is treated as a first-class identity subject within the ecosystem. ChainHub operationalizes this model as the core interoperability layer, enabling secure, granular, and dynamically governed permissions across chains while supporting efficient and controlled interactions. As the coordination layer, ChainHub provides the foundation for unified governance and cross-chain interoperability.

Figure 3: ChainHub Architecture



5.1 Chain-as-Entity Identity Model

Through ChainHub, every Domain Chain receives its own Decentralized Identifier (DID) issued and anchored on the Rootchain. This DID represents the chain itself — independent of its operators, validators, or users — and serves as the primary subject for all authorization decisions.

Key Components:

- DID Registry: A smart contract on the Rootchain that maintains an immutable record of all registered Domain Chain DIDs, including their DID Documents (public keys, endpoints, and metadata).
- Verifiable Credentials (VC): Granular capability credentials issued by the Rootchain that define the exact rights and roles of each Domain Chain. A single chain may hold multiple VCs for different permission scopes (e.g., data submission, settlement participation, or observer role).
- Verifiable Presentations (VP): Signed bundles containing one or more VCs that a Domain Chain presents when interacting with the Rootchain or other chains.

This model allows fine-grained control: permissions can specify allowed operation types, data scopes, rate limits, and validity periods. All credentials are fully auditable on the Rootchain.

5.2 Dual-Gate Runtime Authorization

Every interaction with the Rootchain or critical cross-chain activity undergoes dual-gate validation executed by the Runtime Authorization Engine:

1. Cryptographic Gate: Validates digital signatures and cryptographic state proofs to ensure data integrity and authenticity.
2. Identity & Permission Gate: Resolves the sender's DID from the Registry and verifies the attached VC(s) for validity, revocation status, expiry, and permission match against the requested action.

Only requests that pass both gates are accepted. This mechanism provides strong security guarantees while remaining efficient, as most routine verifications use locally cached or directly presented credentials.

Revocation of a DID or VC takes effect immediately on the next authorization check, enabling real-time response to security incidents or policy changes without system-wide disruption.

5.3 Direct Cross-Chain Interoperability via Verifiable Presentations

NDAChain supports efficient direct peer-to-peer interoperability between Domain Chains, reducing dependency on the Rootchain for every transaction:

- When Domain Chain A wishes to interact with Domain Chain B, Chain A constructs a Verifiable Presentation (VP) containing its relevant VC(s) and signs it with its DID private key.
- Chain B independently verifies two elements:
    - The signature on the VP (confirming the sender's identity via the DID Registry).
    - The embedded VC (confirming the permissions were legitimately issued by the Rootchain).
- If both checks pass, the interaction proceeds directly without querying the Rootchain.

This approach significantly lowers load on the control layer while preserving full national traceability — critical events and state anchors are still recorded on the Rootchain when required for audit or regulatory purposes.

The framework is technology-agnostic: Domain Chains built on different platforms (EVM-compatible, Hyperledger Fabric, custom DLT, Layer 2 rollup solutions) can participate as long as they support DID/VC resolution and VP verification.

5.4 Unified On-Chain and Off-Chain Credential Verification

A major strength of the NDAChain identity framework is its ability to use the same VC seamlessly across environments:

- On-chain: Smart contracts on the Rootchain or Domain Chains verify VPs directly.
- Off-chain: Traditional systems (government portals, enterprise applications, mobile apps, audit tools) can verify VPs by checking signatures against public keys published on the Rootchain — without needing to run a blockchain node.
- Cross-chain: Domain Chains use the same credential format for direct interactions.

This unified approach creates a natural bridge between Web2 and Web3 systems, allowing organizations to maintain a single set of credentials for both blockchain and legacy environments.

5.5 Credential Lifecycle and Governance

The Rootchain manages the full lifecycle of DIDs and VCs through a dedicated Governance Module:

- Issuance: New Domain Chains receive DID and initial VC(s) after whitelist approval.
- Update: Roles, permissions, or constraints can be modified dynamically.
- Restriction / Revocation: Rights can be limited or fully revoked in real time.
- Audit Trail: Every lifecycle event is recorded immutably on the Rootchain.

All governance actions involving high-impact changes are protected by the Trustee Keys (threshold multi-signature) described in Section 4.

6. National Blockchain Adaptation Standard and Integration Kit

The NDAChain Adaptation Standard defines the precise technical and operational requirements that any existing or new Layer 1 blockchain must satisfy to become a fully compliant Domain Chain within the national ecosystem. It serves as the practical bridge between the high-level architectural vision presented in earlier sections and the day-to-day reality of onboarding provincial, ministerial, enterprise, and third-party blockchains. By establishing a clear, versioned national specification, the standard ensures seamless, secure, and technology-agnostic integration while preserving the core consensus mechanisms and business logic of each participating chain. This approach directly addresses one of the key lessons from international initiatives such as China's BSN: a well-defined adaptation layer dramatically accelerates ecosystem growth and reduces integration friction.

The standard applies to a broad range of blockchain technologies, including existing permissioned enterprise platforms (e.g., Besu/Quorum, Hyperledger Fabric), EVM-compatible chains and Layer 2 rollups, Cosmos SDK, and highly customized or hybrid implementations. It explicitly does not require migration of historical data, replacement of native consensus algorithms, or fundamental rewrites of smart-contract logic. Instead, participating chains implement a thin, non-intrusive Adaptation Layer that enables them to inherit national identity, authorization, and auditability from the Rootchain while retaining full operational independence.

To achieve compliance, a blockchain must implement the following core requirements:

1. **Chain-as-Entity Identity**: Register a Decentralized Identifier (DID) issued by the Rootchain DID Registry and maintain a valid DID Document containing public keys and service endpoints.
2. **Credential-Based Authorization** The chain must integrate with the Rootchain credential-based authorization model, where identity and permissions are validated using Verifiable Credentials (VC).
3. **Runtime Trust Reinforcement**: The chain must enforce dual validation for external and cross-chain interactions, with cryptographic verification (signatures / proofs), and identity-based authorization (DID + VC).
4. **Rootchain State Access** The chain must integrate a lightweight client to resolve DID, VC status, and permission data from the Rootchain, with support for local caching.
5. **Anchoring and Auditability Hooks**: Support periodic or event-triggered anchoring of critical state summaries or hashes to the Rootchain.
6. **Standardized Cross-Chain Messaging**: Adopt the official NDAChain cross-chain message schema based on the W3C Verifiable Credentials Data Model v2.0.
7. **Cryptographic and Security Baseline**: Comply with Vietnam's national cryptographic suite and Level 3+ information security requirements.

To minimize effort for chain operators, NDAChain provides an official open-source Adaptation Layer Kit (also referred to as the Integration Kit). This kit acts as a thin but comprehensive integration layer between a participating chain and the Rootchain. This kit includes production-grade components such as the Trust Oracle Client Library (available in Go, Java, JavaScript, and Python), reusable VP verification modules, standardized API Gateway wrappers with built-in rate limiting and dual-gate enforcement, reference smart-contract templates, monitoring and telemetry agents, and deployment scripts. In addition, the Adaptation Layer is responsible for anchoring critical state summaries and proofs from the Domain Chain to the Rootchain, and relaying cross-chain messages and authorization data.

This design allows most chains to integrate by deploying and configuring the Adaptation Layer, without requiring deep modifications to their core protocol or execution engine.

The purely technical integration process for connecting an existing blockchain consists of the following steps:

1. DID registration and publication of the DID Document.
2. Deployment and configuration of the Trust Oracle client.
3. Implementation of VP verification logic and dual-gate authorization.
4. Adoption of standardized anchoring hooks and cross-chain messaging.
5. Local integration testing followed by testnet validation.

For a mature chain using one of the provided reference adapters, pure technical integration typically takes 7–14 days (1–2 weeks).

Reference implementations are already available for the most common frameworks (Hyperledger Fabric, Quorum/Besu, and Cosmos SDK adapters), with additional generic REST/JSON adapters provided for highly customized chains. All source code, documentation, example deployments, and test suites are published in the official NDAChain GitHub repository.

Adoption of the Adaptation Standard brings immediate technical benefits: direct access to national identity services, secure cross-chain data sharing via ChainHub, integration with the NDA Secure File System (NDA SFS), and simplified anchoring to the Rootchain. These capabilities, combined with the open-source kit, enable any Vietnamese blockchain operator to join the national ecosystem efficiently and securely.

The Adaptation Standard will be formally versioned (starting with v1.0 at launch) and maintained by the National Blockchain Steering Committee. Future versions will incorporate emerging cryptographic algorithms, enhanced privacy features (including Zero-Knowledge Proofs), additional framework adapters, and improvements based on real-world ecosystem feedback. By publishing this concrete specification and supporting toolkit, NDAChain transforms the theoretical advantages of the rootchain-centric model into a production-ready national infrastructure that any Vietnamese blockchain operator can join efficiently and securely.

7. Domain Chains and Sector-Specific Execution

While the Rootchain provides unified trust, governance, and oversight, the actual high-volume processing of national services occurs on Domain Chains. These specialized chains enable NDAChain to scale efficiently while meeting the diverse performance and functional requirements of different sectors.

7.1 Purpose and Design Principles

Domain Chains are independent permissioned blockchains optimized for specific national use cases or sectors. They handle the majority of operational workloads, allowing the Rootchain to remain focused on control-plane functions such as identity management, authorization, and auditability.

Key design principles for Domain Chains include:

- Operational Independence: Each Domain Chain can configure its own consensus parameters, block size, and performance tuning to best suit its workload.
- Trust Inheritance: All Domain Chains must register their DID on the Rootchain and receive Verifiable Credentials (VC) defining their permitted roles and operations.
- Controlled Interoperability: Domain Chains interact with each other and the Rootchain through standardized identity-based mechanisms while maintaining national-level oversight.
- Flexibility: Support for both dedicated chains (Blockchain-as-a-Service) and shared chains (Smart Contract-as-a-Service) depending on security, compliance, and performance needs.

This layered separation ensures that high-throughput sector applications do not impact the stability or predictability of national governance functions.

7.2 Types of Domain Chains

NDAChain supports two primary deployment models:

1. Dedicated Domain Chains (Blockchain-as-a-Service - BaaS) Fully independent chains for sectors or organizations requiring strict data isolation, custom governance, or very high transaction volumes. Examples include a national supply chain traceability chain or a healthcare records chain.
2. Shared Domain Chains (Smart Contract-as-a-Service - SCaaS) Multiple applications or sub-sectors share a single chain infrastructure while maintaining logical separation through smart contracts and access controls. This model optimizes cost and simplifies management for lower-volume or related use cases.

Both models must comply with national standards, including mandatory integration with the Rootchain's Trust Oracle and adherence to approved smart contract templates.

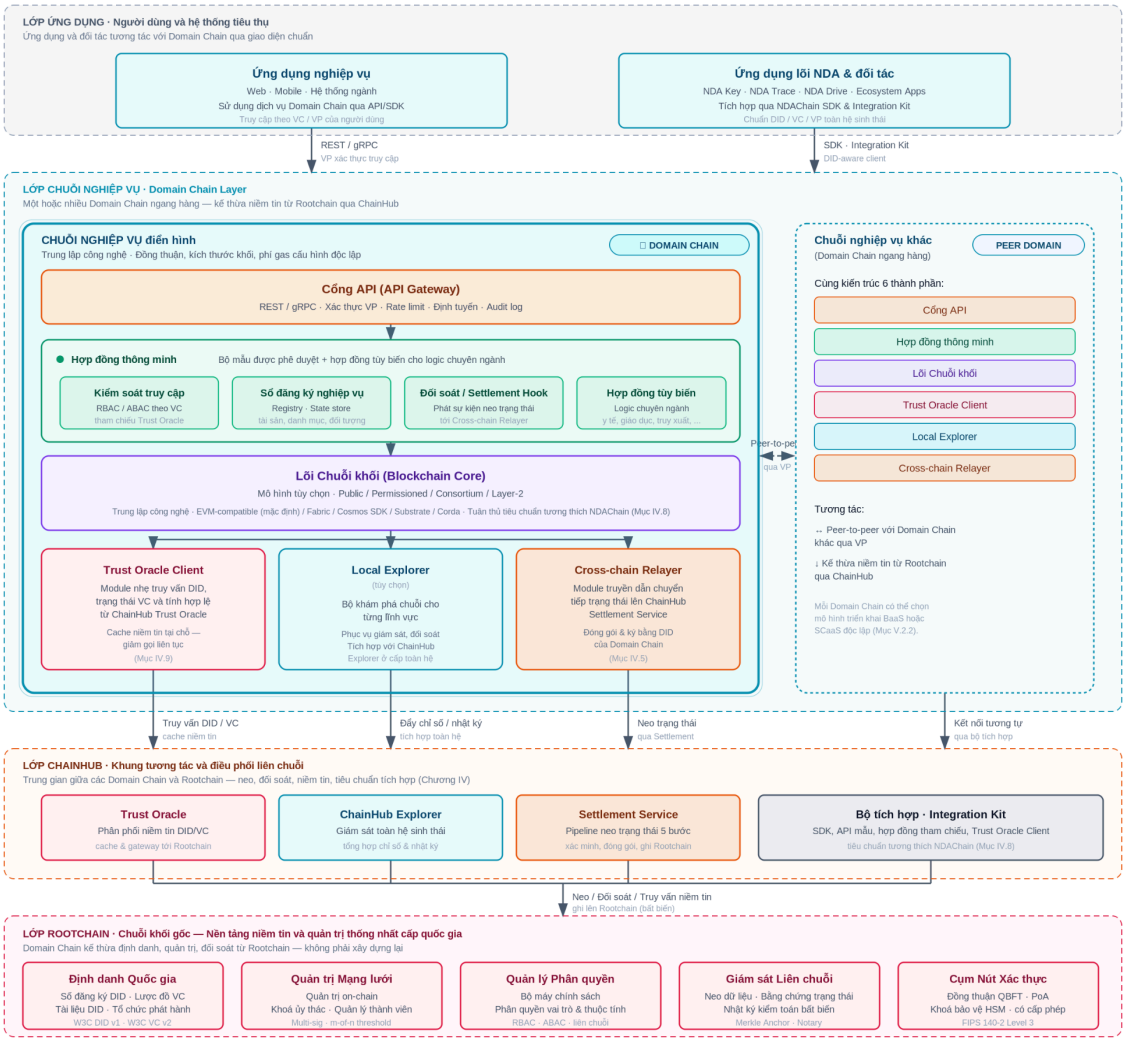
7.3 Architecture of a Domain Chain

Each Domain Chain typically includes the following components:

- Blockchain Core: Permissioned chain (EVM-compatible by default, though other DLT frameworks are supported if they meet interoperability requirements).
- Trust Oracle: A secure bridge service that allows the Domain Chain to query identity, DID status, and VC validity from the Rootchain without constant direct calls. The Oracle caches verified trust information locally for performance.
- Smart Contracts: Pre-approved templates for common functions (access control, registry, auditing) plus custom contracts for sector-specific logic.
- API Gateway: Provides REST/gRPC endpoints with rate limiting and authentication for external applications.
- Local Explorer (optional): Sector-specific blockchain explorer for monitoring and auditing.

Domain Chains connect to the Rootchain primarily through the Trust Oracle for identity and permission checks, and through direct anchoring for critical state updates that require national-level immutability.

Figure 4: Domain Chain Architecture Sample



7.4 Trust Oracle Mechanism

The Trust Oracle acts as a lightweight, event-driven bridge between Domain Chains and the Rootchain. It enables Domain Chains to:

- Verify DID and VC status in real time or from cache.
- Confirm permission scopes before processing transactions.
- Receive revocation notifications with minimal delay.

The Oracle is designed to be resilient and can be implemented in a multi-node decentralized configuration in future phases to further reduce single points of dependency.

7.5 Scaling Benefits

The Domain Chain layer delivers the primary scalability of NDAChain:

- Horizontal Scaling: New Domain Chains can be added quickly for emerging national priorities without impacting existing chains or the Rootchain.
- Vertical Scaling: Individual Domain Chains can be tuned for higher throughput (larger blocks, optimized execution engines, or parallel processing) based on sector demand.
- Load Distribution: Routine high-volume transactions stay on Domain Chains, keeping the Rootchain stable for governance and coordination tasks.

Early deployments have demonstrated that this model allows the overall ecosystem to achieve aggregate throughput well above 100,000 TPS while the Rootchain maintains predictable performance for control operations.

7.6 Current and Planned Domain Chains

NDAChain is already supporting pilot Domain Chains in key areas, including:

- Supply chain and logistics traceability (as demonstrated in early production use cases).
- Digital credential and identity services.
- Secure document and data sharing workflows.

Additional Domain Chains for healthcare, education, financial services, and e-governance are planned in subsequent phases.

By combining the strong governance of the Rootchain with the flexible execution capabilities of Domain Chains, NDAChain provides a scalable and sovereign foundation capable of supporting Vietnam's diverse national digital services both now and in the future.

8. Sovereign Decentralized Storage – NDA SFS

While the blockchain layers provide immutable trust and transaction processing, many national applications require secure, scalable storage of large files, documents, and sensitive data. The NDA Secure File System (NDA SFS) addresses this need by providing a sovereign, decentralized, and identity-centric storage infrastructure that fully aligns with Vietnam's data sovereignty and privacy requirements.

8.1 Objectives and Design Principles

NDA SFS is designed to overcome the limitations of traditional centralized storage systems while ensuring strict compliance with national regulations on data residency and personal data protection (Law 2023 and related decrees).

Core design principles include:

- Data Sovereignty: All data is stored physically within Vietnam's territory across national, regional, and local nodes.
- Identity-Centric Control: Every file or data object is tied to the owner's Decentralized Identifier (DID). Access rights are managed exclusively through Verifiable Credentials (VC) and Verifiable Presentations (VP).
- Zero-Trust Architecture: Data is encrypted end-to-end at the client side before leaving the owner's device. Storage nodes never see plaintext data.
- Privacy by Design: Owners maintain full control over their data, including the ability to grant, restrict, or revoke access instantly.
- High Resilience and Availability: Data is fragmented, encrypted, and distributed with controlled replication across multiple nodes.

8.2 Multi-Tier Storage Architecture

NDA SFS organizes storage into three logical tiers that reflect Vietnam's administrative and operational structure:

- Local Tier (Enterprise / Organizational Nodes): Deployed within government agencies, ministries, hospitals, schools, or enterprises. Provides fast access to frequently used data generated by that organization.
- Regional Tier: Serves as intermediate replication and backup layer across provinces or economic regions. Improves availability and reduces latency for cross-organizational access within the same region.
- National Tier: Long-term archival and disaster recovery layer managed at the national level. Ensures data durability and supports national audit and compliance requirements.

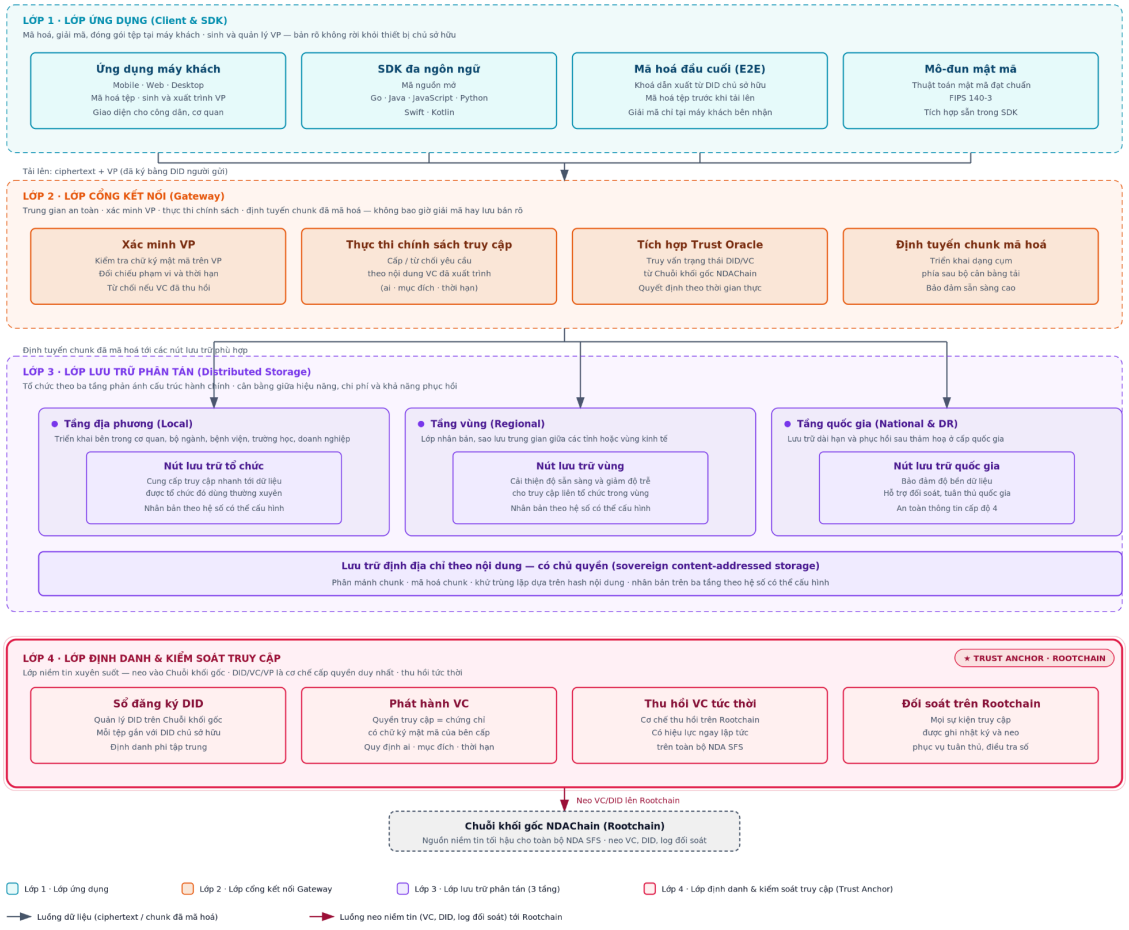
This tiered approach balances performance, cost, and resilience while maintaining unified governance through the Rootchain.

8.3 Key Technical Components

NDA SFS consists of four tightly integrated layers:

1. Identity & Access Control Layer Anchored to the NDAChain Rootchain. Uses DID Registry and VC/VP mechanisms to manage all access rights. Every file is associated with the owner's DID, and permissions are expressed as cryptographically signed credentials.
2. Application Layer Client-side applications and SDKs handle encryption, decryption, and packaging of data. Files are encrypted using keys derived from the owner's DID before upload. The application also generates and manages VPs when granting or proving access.
3. Gateway Layer Stateless gateways act as secure intermediaries. They verify VP credentials, enforce access policies, and route encrypted data to the appropriate storage nodes. Gateways never decrypt or store plaintext data.
4. Distributed Storage Layer Built on content-addressable storage (similar to IPFS principles but fully sovereign and controlled). Data is split into encrypted chunks, deduplicated via content hashing, and distributed with configurable replication factors across the three tiers.

Figure 5: NDA SFS Architecture



8.4 Data Access and Sharing Flow

The secure data sharing process follows these steps:

1. Upload & Encryption: The data owner encrypts the file locally using DID-derived keys and uploads the ciphertext to NDA SFS via the gateway.
2. Permission Granting: The owner issues a Verifiable Credential (VC) specifying access rights (who can access, for what purpose, and for how long) and sends it to the authorized party.
3. Access Request: The recipient presents a Verifiable Presentation (VP) signed with their own DID to prove ownership of the granted VC.
4. Verification & Retrieval: The gateway verifies the VP against the Rootchain, then routes the encrypted chunks to the recipient's application.

5. Client-Side Decryption: Only the authorized recipient's application can decrypt the data using the appropriate keys.

This flow ensures that storage nodes remain completely blind to content, while access control stays fully decentralized and auditable.

8.5 Security and Compliance Features

- End-to-End Encryption: Data is encrypted before leaving the owner's device and remains encrypted at rest and in transit.
- Zero-Trust Model: No single node or operator can access plaintext data.
- Real-Time Revocation: Revoking a VC immediately prevents further access on subsequent requests.
- Auditability: All access events can be logged and anchored to the Rootchain for compliance and forensic purposes.
- National Compliance: Fully supports data residency, personal data protection laws, and national security requirements (including Level 4 information security standards).

8.6 Strategic Value

NDA SFS completes the NDAChain vision by providing a secure, sovereign storage foundation that works seamlessly with the blockchain layers. It enables safe sharing of large documents, certificates, medical records, educational credentials, and other sensitive data across government agencies and with citizens — all while maintaining strict owner control and national oversight.

Together with the Rootchain and Domain Chains, NDA SFS forms a complete sovereign infrastructure capable of supporting Vietnam's most demanding digital transformation initiatives.

9. Security, Privacy, and Resilience

NDAChain is designed as a national critical infrastructure, requiring the highest standards of security, privacy, and operational resilience. Security is not treated as an add-on but embedded throughout the architecture through a Security-by-Design and Privacy-by-Design approach, aligned with Vietnam's Level 4 information security requirements and international best practices.

9.1 Security Architecture Overview

NDAChain adopts a Zero-Trust security model across all layers. No entity — whether a Domain Chain, node operator, or application — is inherently trusted. Every request must be explicitly authenticated and authorized using cryptographic proofs and identity credentials.

Key security principles include:

- Least Privilege: Permissions are granular and time-bound through Verifiable Credentials (VC).
- Defense in Depth: Multiple independent security controls at infrastructure, blockchain, identity, storage, and application layers.
- Immutable Auditability: All critical actions, governance decisions, and access events are recorded on the Rootchain.
- Real-Time Revocation: Compromised identities or credentials can be revoked instantly with immediate system-wide effect.

9.2 Multi-Layer Security Controls

Infrastructure Layer

- Validators and nodes are deployed in secure national data centers with geographic redundancy across North, Central, and South regions.
- Network access is restricted through IP whitelisting, mutual TLS (mTLS), and P2P protocol-level encryption.
- All external-facing services are protected by Web Application Firewall (WAF), DDoS mitigation, and strict rate limiting.

Rootchain and Governance Layer

- Proof-of-Authority (PoA) with QBFT consensus limits participation to pre-approved, high-trust validators.
- Critical governance actions are protected by Trustee Keys using threshold multi-signature (m-of-n) schemes stored in Hardware Security Modules (HSMs).
- All upgrades, validator changes, and emergency interventions require explicit multi-party approval and are permanently logged on-chain.

Identity and Authorization Layer

- Dual-gate validation (cryptographic proof + identity/permission check) for every sensitive operation.
- Real-time DID and VC revocation through an on-chain revocation registry.
- Support for quantum-resistant cryptography options in future upgrades.

Storage Layer (NDA SFS)

- End-to-end encryption performed at the client side before data leaves the owner's device.
- Storage nodes only handle encrypted fragments and have no access to decryption keys.
- Access is strictly controlled through DID-signed Verifiable Presentations (VP).

Application Layer

- All client applications use secure SDKs that enforce encryption and credential-based authentication.
- Sensitive operations require explicit user or system consent via VC issuance.

9.3 Privacy Protection

NDAChain strongly protects personal and sensitive data through:

- Self-Sovereign Identity: Individuals and organizations control their own DIDs and decide what information to share via selective disclosure mechanisms (supported by Zero-Knowledge Proofs where applicable).
- Minimal Data Disclosure: Verifiable Credentials allow proving specific attributes (e.g., "over 18" or "authorized logistics provider") without revealing unnecessary personal data.
- Data Residency: All blockchain state and storage nodes operate exclusively within Vietnam's territory.
- Separation of Concerns: The Rootchain stores only minimal metadata (DIDs and public keys), while actual sensitive content remains encrypted in NDA SFS under owner control.

9.4 Resilience and High Availability

NDAChain is engineered for continuous operation even under adverse conditions:

- Geographic Redundancy: Validators and storage nodes are distributed across three major regions to survive regional outages or natural disasters.
- Fault Tolerance: The Rootchain's QBFT consensus tolerates up to one-third faulty or compromised validators.
- Automated Failover: Nodes automatically reconnect and resynchronize in case of network partitions.
- Disaster Recovery: Regular backups, snapshots, and tested Business Continuity Plans (BCP) ensure rapid recovery.
- Target Availability: ≥ 99.95% system uptime, validated through extended testnet and early production operations.

Table 2: Key Security and Resilience Features

Aspect	Mechanism	Benefit
Consensus Security	QBFT PoA + Threshold Trustee Keys	Controlled participation with emergency override

Aspect	Mechanism	Benefit
Authorization	Dual-gate (Crypto + Identity) Validation	Strong protection against unauthorized access
Data Protection	Client-side E2EE + Zero-Trust Storage	Storage nodes cannot access plaintext
Revocation	Real-time on-chain revocation registry	Immediate effect across the ecosystem
Resilience	3-region distribution + 1/3 fault tolerance	Survives regional failures
Auditability	Immutable Rootchain logging	Full regulatory and forensic traceability

9.5 Compliance and Certification

NDAChain is built to comply with:

- National information security Level 4 requirements.
- Personal Data Protection Law and data residency regulations.
- International standards including W3C DID/VC, ISO/IEC 27001, and eIDAS 2.0 principles (where applicable under national control).

Regular independent security audits, penetration testing, and compliance assessments are conducted as part of the ongoing governance process.

By integrating strong technical controls with robust governance and national oversight, NDAChain delivers a secure, private, and highly resilient foundation capable of supporting Vietnam's most sensitive digital services.

9.6 Quantum Resistance and Cryptographic Agility

NDAChain is designed as a long-term national trust infrastructure and incorporates a forward-compatible approach to cryptographic security, including preparedness for potential quantum computing threats.

Current Capabilities

The current implementation already includes foundational support for post-quantum readiness:

- Dual-Signature Block Mechanism (Optional Mode):
  NDAChain code supports an optional mode in which blocks can be signed using both a classical signature scheme (e.g., ECDSA) and post-quantum algorithm aligned with emerging standards ML-DSA (FIPS 204). This enables early adoption of quantum-resistant security while maintaining compatibility with existing infrastructure. This mechanism is initially deployed in selected Domain Chains to validate performance and interoperability, ahead of broader adoption in the Rootchain.
- Identity Layer Flexibility:
  The DID and Verifiable Credential (VC) framework supports multiple cryptographic methods, allowing identity issuers to adopt stronger algorithms without changes to the underlying chain.

Design Principles

- Cryptographic Agility: Algorithms are not fixed and can be upgraded through standard identifiers in DID and verification processes.
- Layered Migration: Rootchain, ChainHub, and Domain Chains can adopt post-quantum mechanisms independently.
- Hybrid Transition Model: Dual-signature approaches ensure continuity of trust during migration phases.

Forward Path

NDAChain will continue to align with international post-quantum standards and gradually expand quantum-resistant cryptography across identity, governance, and cross-chain authorization components.

10. Governance, Operations, and Ecosystem Management

Effective governance is essential for a national blockchain infrastructure. NDAChain implements a clear, layered governance framework that ensures strong state oversight, operational efficiency, and broad ecosystem participation while maintaining transparency and accountability.

10.1 Governance Principles

NDAChain's governance follows three core principles derived from national requirements:

- Unified National Control: The Rootchain serves as the single authoritative layer for strategic decisions and policy enforcement.
- Separation of Duties: Clear distinction between policy setting, service management, and day-to-day operations to prevent concentration of power and enable effective oversight.
- Auditable Transparency: All governance actions, especially those involving Trustee Keys, are permanently recorded on the Rootchain for audit and regulatory review.

10.2 Three-Layer Governance Model

NDAChain adopts a structured three-layer governance framework:

1. Governance Layer (Policy and Strategic Oversight)

- Led by the National Blockchain Steering Committee (or designated national authority).
- Responsible for high-level policy, major architecture decisions, approval of new Domain Chains, and setting national standards.
- Key mechanism: Trustee Keys (threshold multi-signature) held by a small group of designated national trustees. These keys are required for critical actions such as protocol upgrades, emergency interventions, validator set changes, or large-scale policy enforcement.
- All Trustee Key actions are mandatorily logged on the Rootchain with full cryptographic proof.

2. Management Layer (Service and Quality Oversight)

- Responsible for day-to-day service quality, standards compliance, SLA management, and ecosystem coordination.
- Key functions include:
    - Defining technical standards and integration requirements.
    - Managing Service Level Agreements (SLAs) with participating organizations.
    - Overseeing security compliance and risk management.
    - Coordinating cross-sector interoperability.

This layer acts as the bridge between strategic policy and technical operations.

3. Operations Layer (Technical Implementation and Maintenance)

- Handles the actual running, monitoring, and technical evolution of the infrastructure.
- Key responsibilities:
    - Validator node deployment and maintenance.
    - Network monitoring and incident response (24/7 NOC and SOC).
    - Domain Chain deployment and support (BaaS and SCaaS models).
    - Technical upgrades and performance optimization.
    - Onboarding new participants and providing technical assistance.

10.3 Trustee Keys and Emergency Governance

The Special Administrative Keys (Trustee Keys) provide a powerful yet controlled mechanism for national authorities:

- Enable rapid intervention in emergencies (e.g., security incidents, chain suspension, or critical policy enforcement).
- Require multi-party approval (threshold scheme) to prevent unilateral action.
- Ensure every use is fully auditable on the Rootchain, balancing speed with accountability.

This mechanism is particularly valuable for a national infrastructure, allowing swift response while preserving trust and transparency.

10.4 Validator and Participant Onboarding

Participation in NDAChain is strictly controlled:

- Validator Nodes: Selected through a transparent national process based on technical capability, legal standing, and strategic importance. Only approved organizations (ministries, major state enterprises, and trusted technology providers) may run validators.
- Operating Nodes: Broader participation allowed for data synchronization and querying.
- Domain Chain Operators: Any approved government agency or enterprise can request a dedicated or shared Domain Chain after successful DID registration and VC issuance.

The onboarding process includes technical assessment, security audit, and formal approval via the Governance Layer.

10.5 Operational Model

NDAChain operates with a clear division of responsibilities:

- 24/7 Monitoring: Centralized Network Operations Center (NOC) and Security Operations Center (SOC) for real-time oversight.
- Incident Response: Defined escalation procedures with clear ownership at each governance layer.
- Performance Management: Regular reporting on key metrics including Rootchain TPS, ecosystem throughput, finality time, and system availability.
- Upgrade Process: Controlled through smart contract governance with mandatory Trustee Key approval for major changes.

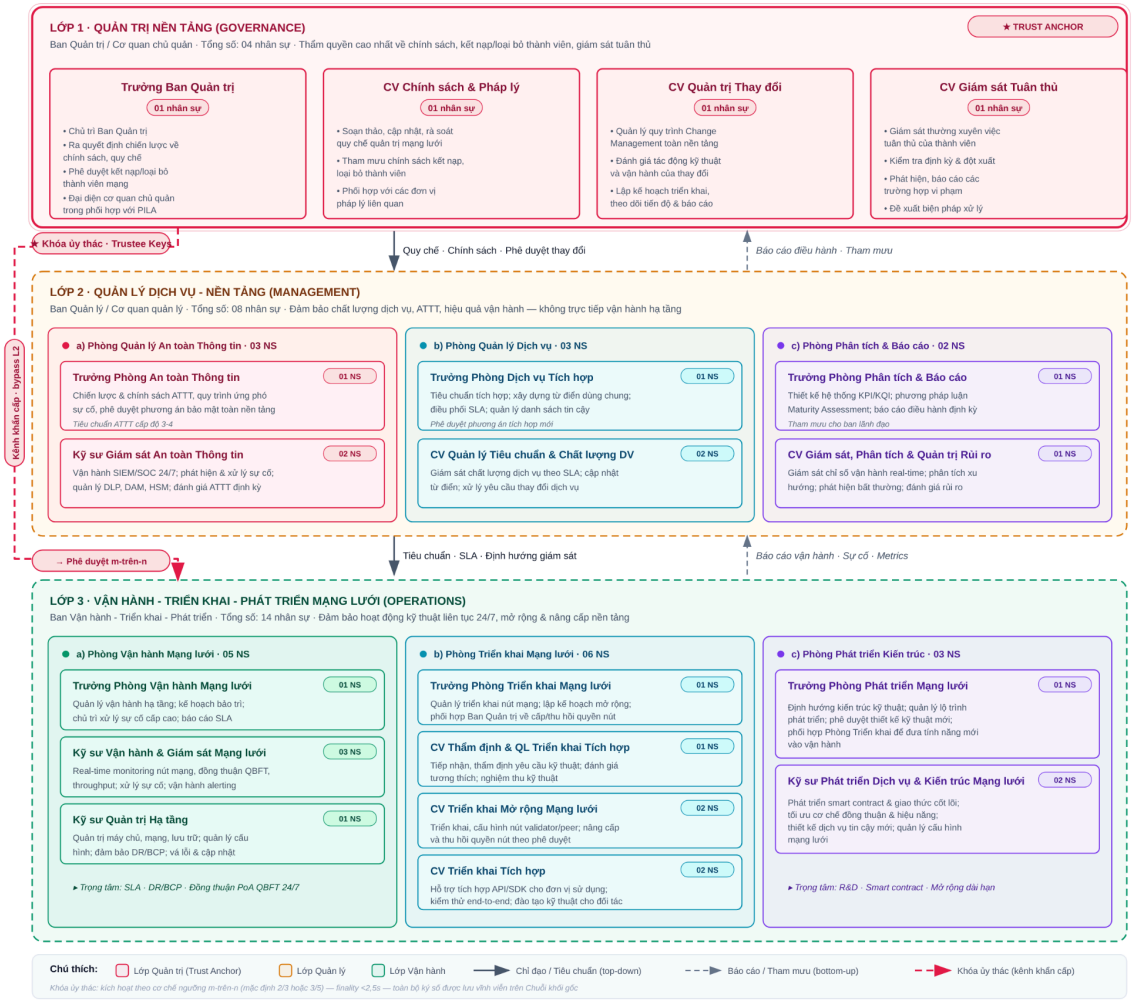
Gas-free operations for public services are funded at the national infrastructure level, encouraging widespread adoption across government agencies and citizens.

10.6 Ecosystem Development

NDAChain actively fosters a vibrant national ecosystem through:

- Developer Tools: EVM-compatible environment, SDKs, and pre-approved smart contract templates.
- Integration Support: API gateways, documentation, and technical assistance for ministries and enterprises.
- Pilot Programs: Ongoing deployment of Domain Chains in priority sectors (supply chain, digital credentials, secure document sharing).
- Training and Capacity Building: Programs to develop national blockchain expertise.

Figure 6: NDAChain Three-Layer Governance Model



This governance framework ensures that NDAChain remains under strong national control while remaining flexible enough to support innovation and broad participation across Vietnam's digital economy.

11. Implementation Status and Performance

NDAChain has moved beyond theoretical design into active development, testing, and early production deployment. This section presents the current implementation status, real-world performance metrics, and initial results from prototypes, national testnet, and pilot use cases.

11.1 Current Implementation Status

NDAChain is currently operational in three environments:

- Prototype Environment: Small-scale setup used for initial architecture validation and feature development.
- National Testnet: Full-scale environment with validators distributed across North, Central, and South regions. This serves as the primary testing and benchmarking platform.
- Early Production Deployments: Limited production use with real national workloads, most notably in supply chain and logistics traceability.

The Rootchain is fully implemented, deployed, and rolled out in production. The identity and interoperability framework (DID Registry, VC issuance, Runtime Authorization Engine, and Verifiable Presentation support) is deployed and functional. Multiple Domain Chains have been successfully connected, and the NDA Secure File System (NDA SFS) is operational in pilot mode.

Key components already in production or advanced testing include:

- Rootchain governance and Trustee Key mechanisms
- Chain-as-Entity DID registration and VC lifecycle management
- Dual-gate runtime authorization

- Direct Domain Chain-to-Domain Chain interoperability via VP
- Multi-tier NDA SFS with end-to-end encryption

11.2 Performance Results

Real-world benchmarks conducted on the national testnet and early production environment demonstrate that NDAChain meets or exceeds its design targets.

Rootchain (Control Layer) Performance:

- Sustained write throughput: 1,150 – 1,280 TPS under mixed governance, DID/VC issuance, and cross-chain anchoring workloads.
- Average finality: 2.1 – 2.4 seconds (deterministic).
- Block time: 2.5 seconds (± 0.2 s) as configured.
- Resource efficiency: Stable operation with 7–11 validators distributed across three geographic regions.
- Uptime: 99.97% achieved during extended 72+ hour stress tests.

Ecosystem-Wide Performance:

- Aggregate throughput across Domain Chains: Exceeding 100,000 TPS when running multiple concurrent Domain Chains.
- Cross-chain interaction overhead using Verifiable Presentations: Less than 8% additional latency compared to local Domain Chain transactions.
- NDA SFS retrieval latency: Sub-second for local-tier access; under 2 seconds for regional/national-tier access under normal load.

These results confirm the effectiveness of the layered architecture: the Rootchain remains stable and predictable for governance tasks, while Domain Chains absorb the bulk of high-volume operational workloads.

Table 3: NDAChain Performance Summary (Testnet & Early Production)

Metric	Rootchain (Control)	Ecosystem (Domain Chains)	Notes
Write Throughput	1,150 – 1,280 TPS	> 100,000 TPS aggregate	Mixed real workloads
Finality	2.1 – 2.4 seconds	< 5 seconds (anchored)	Deterministic on Rootchain
Block Time	2.5 seconds	Configurable per chain	—
Uptime	99.97%	99.95%+	Measured over 30+ days
Cross-chain VP Overhead	—	< 8%	Direct Domain-to-Domain

11.3 Pilot Use Cases

The first production pilot involves a Logistics and Supply Chain Traceability Domain Chain connected to the Rootchain:

- Events (production, transportation, distribution) are recorded on the Domain Chain.
- Critical traceability anchors and ownership transfers are submitted to the Rootchain for national-level verification and auditability.
- Participating organizations use Verifiable Presentations for direct data exchange between authorized chains.

- NDA SFS is used to securely store supporting documents (certificates, invoices, inspection reports) with owner-controlled access.

Early results show significant improvements in traceability speed, reduced fraud risk, and simplified compliance reporting for regulatory authorities.

Additional pilots in digital credentials and secure government document sharing are underway and showing promising results.

11.4 Lessons Learned and Ongoing Optimization

Implementation has validated several architectural choices:

- The separation of control plane (Rootchain) and execution plane (Domain Chains) effectively prevents governance bottlenecks.
- Direct VP-based interoperability significantly reduces Rootchain load.
- Geographic distribution of validators provides excellent resilience.
- Trustee Key mechanism enables fast, auditable emergency governance.

Areas under continuous optimization include further tuning of the Trust Oracle for lower latency, expansion of NDA SFS replication strategies, and refinement of monitoring dashboards for ecosystem-wide visibility.

NDAChain's phased implementation approach — starting with core Rootchain stability, then expanding Domain Chains and storage — has proven effective for risk management and steady capability growth.

The current status confirms that NDAChain is not only theoretically sound but practically viable as Vietnam's national blockchain foundation, delivering measurable performance and real operational value in priority sectors.

12. Comparative Analysis and Strategic Advantages

NDAChain's rootchain-centric hierarchical multichain architecture is specifically tailored to Vietnam's context as a mid-sized unitary state. This section compares it with major international approaches and highlights its strategic advantages.

12.1 Comparison with International Models

National blockchain initiatives worldwide have adopted different architectural philosophies depending on scale, governance model, and priorities:

- China's Blockchain-based Service Network (BSN): A large-scale federated "network of networks" without a single technical root. It achieves massive scale through standardization and policy coordination but offers relatively loose technical traceability and centralized control across thousands of chains.
- European Union's European Blockchain Services Infrastructure (EBSI): A peer-to-peer permissioned network emphasizing cross-border interoperability and self-sovereign identity. It deliberately avoids a central technical root to respect member state sovereignty, resulting in complex coordination and limited unified auditability.
- India's National Blockchain Framework (Vishvasya): A distributed Blockchain-as-a-Service model focused on public services. While governed at the policy level through centralized cloud resources, it lacks a single authoritative control layer for consistent cross-chain governance and traceability.

In contrast, NDAChain adopts a rootchain-centric hierarchical model with a permissioned Rootchain serving as the central trust and control anchor. This design is particularly well-suited to Vietnam's scale (approximately 100 million population) and unitary governance structure, where strong national oversight and efficient policy enforcement are strategic priorities.

12.2 Key Comparative Advantages

1. Stronger Unified Governance and Auditability

NDAChain provides a single authoritative Rootchain where all critical decisions — whitelist management, identity anchoring, permission issuance, and cross-chain activities — are logged with cryptographic proof-of-control. This delivers immediate, national-level auditability that is difficult to achieve in federated or peer-to-peer models, where traceability remains distributed and coordination-intensive.

2. Balanced Control and Scalability

The layered architecture cleanly separates the control plane (Rootchain) from the execution plane (Domain Chains). The Rootchain maintains predictable performance (~1,200 TPS write throughput with ≤ 2.5 seconds finality), while Domain Chains deliver high aggregate throughput (> 100,000 TPS ecosystem-wide). This enables both horizontal scaling (adding new Domain Chains) and vertical scaling (tuning individual chains) without compromising national oversight.

3. Efficient and Responsive Governance

Special Administrative Keys (threshold multi-signature) allow designated national trustees to perform rapid emergency interventions while ensuring all actions remain fully auditable on the Rootchain. Chain approval, permission updates, and revocations can be executed in minutes to hours, compared to days or weeks of policy coordination in larger federated systems.

4. Fewer Attack Surfaces and Simpler Security

By concentrating control in one well-protected Rootchain layer rather than hundreds of independent nodes, NDAChain has significantly fewer primary attack surfaces. Combined with dual-gate validation, real-time revocation, and geographic distribution, this results in a simpler and more enforceable security model.

5. Technology-Agnostic Interoperability

Domain Chains can join the ecosystem regardless of their underlying technology (EVM, Hyperledger Fabric, custom chains, Layer 2, sidechains, or appchains). Direct peer-to-peer interactions via Verifiable Presentations further reduce central bottlenecks while preserving traceability.

6. Sovereign Data Storage and Web2–Web3 Bridge

The NDA Secure File System (NDA SFS) provides end-to-end encrypted, identity-centric storage with multi-tier national distribution. The same Verifiable Credentials work seamlessly for both on-chain and off-chain verification, creating a natural bridge between traditional systems and blockchain applications.

12.3 Quantitative Comparison

Table 4: NDAChain vs Major National Blockchain Initiatives

Aspect	NDAChain (Vietnam)	BSN (China)	EBSI (EU)	Vishvasya (India)
Architecture	Rootchain-centric hierarchical	Federated network	Peer-to-peer federation	Distributed BaaS
Control Mechanism	Strong technical + policy	Policy + standardization	Decentralized among states	Policy + cloud
Traceability & Auditability	High (single source on Rootchain)	Distributed	Distributed	Moderate
Optimal Scale	Mid-sized unitary states	Very large	Multi-sovereign union	Large federal
Governance Responsiveness	High (minutes–hours)	Medium–high	Low–medium	Medium
Attack Surfaces	Low (central control layer)	High	High	Medium

Aspect	NDAChain (Vietnam)	BSN (China)	EBSI (EU)	Vishvasya (India)
Technology Flexibility	High (agnostic)	Medium	Medium	Medium

12.4 Strategic Advantages for Vietnam

For a country of Vietnam's scale and governance model, the rootchain-centric approach offers a pragmatic balance:

- It delivers clearer accountability and faster national response than highly decentralized models.
- It avoids the performance limitations of a single chain and the coordination overhead of large federations.
- It strongly supports digital sovereignty, data residency, and unified policy enforcement — core goals of the National Blockchain Strategy.
- It provides a future-proof foundation that can scale with national needs while remaining firmly under Vietnamese control.

NDAChain therefore represents not just a technical solution, but a strategically aligned national infrastructure that positions Vietnam to lead in sovereign blockchain development among mid-sized unitary states.

13. Conclusion

NDAChain represents Vietnam's strategic effort to build a sovereign national blockchain infrastructure capable of meeting the demands of the digital age. By adopting a rootchain-centric hierarchical multichain architecture, the platform successfully brings together strong centralized governance and national oversight with the flexibility and scalability needed for a wide range of sector-specific applications.

At its core, the permissioned Rootchain functions as the central trust anchor and control layer for the entire ecosystem. It handles national-level identity management through Decentralized Identifiers (DID), enforces permissions using Verifiable Credentials (VC), and ensures real-time authorization and auditability for all critical operations. Specialized Domain Chains manage the bulk of high-volume sector workloads independently, while the NDA Secure File System (NDA SFS) provides sovereign, end-to-end encrypted storage with identity-centric access control. Direct interoperability between Domain Chains, enabled by Verifiable Presentations (VP), further improves efficiency without sacrificing national traceability.

Real-world testing and early deployments have confirmed the practicality of this design. The Rootchain consistently achieves around 1,200 write transactions per second with deterministic finality in under 2.5 seconds. At the ecosystem level, aggregate throughput across multiple Domain Chains exceeds 100,000 TPS. The geographic distribution of validators across Vietnam's three main regions (North, Central, and South), combined with threshold-based Trustee Keys for emergency governance and zero-base-fee operations for public services, shows that NDAChain can deliver both strong control and solid operational performance.

This architecture is especially well-suited to Vietnam as a mid-sized unitary state. It offers clearer accountability and faster policy enforcement than large-scale federated systems such as China's BSN or the EU's EBSI, while avoiding the scalability limitations of single-chain approaches. By closely aligning with the National Blockchain Strategy outlined in Decision 1236/QĐ-TTg (2024) and other national digital frameworks, NDAChain establishes a secure and controllable foundation for key national services including digital identity, secure data sharing, supply chain traceability, and e-governance.

Looking forward, NDAChain will evolve through the phased rollout of additional Domain Chains, stronger privacy enhancements, deeper integration with existing national digital platforms, and cautious exploration of controlled international interoperability — always under full national oversight. Beyond supporting Vietnam's own digital transformation, the platform has the potential to serve as a practical reference model for other countries facing similar scale and governance challenges.

In essence, NDAChain reflects Vietnam's commitment to technological self-reliance and digital sovereignty. It shows that a balanced, hierarchical approach — strong governance at the center and flexible execution at the edges — can successfully deliver the control, scalability, and innovation needed to build a trusted digital nation for the future.