GOVERNMENT OF THE PEOPLE'S REPUBLIC OF BANGLADESH

Ministry of Posts, Telecommunications and Information Technology
Information and Communication Technology Division

NATIONAL BLOCKCHAIN POLICY
OF BANGLADESH
2026

V. 1.0

January 2026

Table of Contents

ACRONYMS AND ABBREVIATIONS

Acronym	Full Form
AML	Anti-Money Laundering
API	Application Programming Interface
BCC	Bangladesh Computer Council
BDCCL	Bangladesh Data Centre Company Limited
BIFT	Bangladesh Institute of ICT in Development
BNDIA	Bangladesh National Digital Infrastructure Architecture
BSEC	Bangladesh Securities and Exchange Commission
CBDC	Central Bank Digital Currency
CDO	Chief Data Officer
CFT	Combating the Financing of Terrorism
CII	Critical Information Infrastructure
CSO	Cyber Safety Ordinance, 2025
DA	Data Availability
DAO	Decentralized Autonomous Organization
DApp	Decentralized Application
DeFi	Decentralized Finance
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DPoS	Delegated Proof of Stake
DR	Disaster Recovery
DRA	Data Resharing Agreement
DvP	Delivery versus Payment
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
E-KYC	Electronic Know Your Customer
EVM	Ethereum Virtual Machine
FIPS	Federal Information Processing Standards
GRS	Grievance Redress System
HSM	Hardware Security Module
HTLC	Hash Time-Locked Contract
IAM	Identity and Access Management
IBC	Inter-Blockchain Communication
ICT	Information and Communication Technology

IPFS	InterPlanetary File System
ISO	International Organization for Standardization
KYC	Know Your Customer
L2	Layer 2
MEV	Maximal Extractable Value
MFA	Multi-Factor Authentication
MFS	Mobile Financial Services
MPC	Multi-Party Computation
NBI	National Blockchain Infrastructure
NBTC	National Blockchain Technical Committee
NCERT	National Cyber Emergency Response Team
NCSA	National Cybersecurity Agency
NDC	National Data Center
NDE	National Datacentre Ecosystem
NDGA	National Data Governance Authority
NDGO	National Data Governance Ordinance, 2025
NID	National Identity
NRDEX	National Responsible Data Exchange
NSOC	National Security Operations Center
PBFT	Practical Byzantine Fault Tolerance
PDPO	Personal Data Protection Ordinance, 2025
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoA	Proof of Authority
PoS	Proof of Stake
PPP	Public-Private Partnership
RBAC	Role-Based Access Control
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDG	Sustainable Development Goals
SID	Sectoral Identifier
SIEM	Security Information and Event Management
SITA	System Integration for Trusted Access
SOP	Standard Operating Procedure
SSI	Self-Sovereign Identity
SSO	Single Sign-On
STAR	Secure Trusted Architecture for Responsible Exchange

TLS	Transport Layer Security
TPS	Transactions Per Second
TRUST-CCA	Trust and Certificate Chain Authority
VAPT	Vulnerability Assessment and Penetration Testing
VASP	Virtual Asset Service Provider
VC	Verifiable Credential
VID	Virtual Identifier
VP	Verifiable Presentation
W3C	World Wide Web Consortium
WAF	Web Application Firewall
WCAG	Web Content Accessibility Guidelines
ZKP	Zero-Knowledge Proof
ZK-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
ZK-STARK	Zero-Knowledge Scalable Transparent Argument of Knowledge

KEY TERMS AND DEFINITIONS

Attestation

A signed statement asserting a fact, such as eligibility or event occurrence. Attestation services issue cryptographically signed statements about events or data that can be verified by third parties without requiring trust in a central authority.

Atomic Settlement

A settlement mechanism where the transfer of an asset and payment occur simultaneously or not at all. This eliminates counterparty risk by ensuring that both parties to a transaction receive what they are owed, or neither party receives anything, thereby preventing situations where one party fulfils their obligation while the other defaults.

Atomic Swap

A cryptographic mechanism enabling two parties to exchange assets across different blockchain networks without trusting an intermediary, typically using Hash Time-Locked Contracts (HTLCs). This technique ensures that either both parties receive their exchanged assets or neither does, eliminating the need for trusted third parties in cross-chain transactions.

Block

A data structure in a blockchain containing a batch of transactions, a reference (hash) to the previous block, a timestamp, and consensus-related metadata. Blocks are cryptographically linked in sequential order to form an immutable chain of records.

Block Header

The portion of a block containing metadata used for validation and linking, including the previous block hash, Merkle root of transactions, timestamp, and consensus fields. The header hash serves as the unique identifier for the block and is essential for maintaining the chain's integrity.

Blockchain

A distributed ledger where transactions are grouped into blocks that are cryptographically linked and replicated across multiple nodes in a peer-to-peer network. Depending on the design, a blockchain can be permissionless (open participation by any party) or permissioned (controlled participation by authorized entities only). The technology provides properties of immutability, transparency, and decentralized consensus.

Byzantine Fault Tolerance (BFT)

The property of a distributed system that enables it to reach consensus despite the presence of malicious or faulty nodes. BFT consensus protocols, such as Practical Byzantine Fault Tolerance (PBFT), can tolerate up to one-third of participating nodes being compromised or behaving arbitrarily while still guaranteeing correct operation.

Central Bank Digital Currency (CBDC)

A digital form of sovereign currency issued by a central bank, distinct from private cryptocurrencies or stablecoins. CBDCs represent a liability of the central bank and maintain the same monetary sovereignty as physical currency while enabling programmable, traceable, and efficient digital transactions.

Consensus Mechanism

The protocol by which distributed nodes in a blockchain network agree on the canonical ledger state, including the ordering of transactions and block production rules. Consensus mechanisms determine the security assumptions, energy and resource footprint, performance characteristics, and governance model of a blockchain system. Common mechanisms include Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA).

Crypto-Shredding

A technique for achieving effective data erasure by securely deleting encryption keys, rendering encrypted data permanently inaccessible without breaking blockchain integrity. This approach is essential for compliance with data protection regulations such as the Right to Erasure, as it allows organizations to make personal data stored off-chain unrecoverable while maintaining the validity of on-chain hash references.

Cryptographic Hash Function

A one-way mathematical function that maps input data of arbitrary size to a fixed-length output (digest) in a deterministic manner. Hash functions are designed to be collision-resistant (computationally infeasible to find two different inputs producing the same output) and preimage-resistant (computationally infeasible to derive the input from the output). They are fundamental to blockchain integrity, digital signatures, and data verification.

Data Availability

The guarantee that transaction data needed to reconstruct and verify blockchain state is publicly accessible to all network participants. In Layer 2 systems, data availability is a critical security assumption, as users must be able to access the underlying data to independently verify state transitions and exercise their rights to exit the system.

Decentralized Application (DApp)

An application whose backend logic runs fully or partially on decentralized infrastructure such as smart contracts deployed on a blockchain, with frontends often hosted on traditional web servers or decentralized storage systems. DApps combine the benefits of decentralized execution with user-friendly interfaces.

Decentralized Autonomous Organization (DAO)

An organization governed by rules encoded in smart contracts, where decisions are made through token-based voting or other on-chain governance mechanisms. DAOs operate without traditional hierarchical management structures and enable transparent, programmable collective decision-making.

Decentralized Finance (DeFi)

Financial services delivered through smart contracts on blockchain networks, including lending, borrowing, trading, and derivatives, often without traditional intermediaries such as banks or brokerages. DeFi protocols enable permissionless access to financial services but raise significant regulatory considerations regarding consumer protection, market integrity, and anti-money laundering compliance.

Decentralized Identifier (DID)

A globally unique identifier format that enables entities to prove control over their identifiers using cryptographic keys, without relying on centralized registration authorities. DIDs are typically described by a DID Document containing public keys and service endpoints. The W3C DID specification provides the foundation for interoperable self-sovereign identity systems.

Digital Public Infrastructure (DPI)

Shared, population-scale digital building blocks such as digital identity platforms, payment gateways, and data exchange frameworks, implemented with open standards and public governance. DPI enables inclusive, efficient, and secure delivery of public and private services at national scale.

Distributed Ledger Technology (DLT)

A broader class of distributed data structures where multiple parties maintain a synchronized ledger without a single central database. Blockchain is one subtype of DLT; other variants include directed acyclic graphs (DAGs) and other consensus-based distributed data structures. DLT enables technology-neutral regulation covering various implementation approaches.

Finality

The guarantee that a transaction, once confirmed, cannot be reversed, altered, or removed from the blockchain. Finality can be probabilistic (increasing confidence over time as more blocks are added) or deterministic (immediate and absolute upon confirmation). The type of finality depends on the consensus mechanism employed.

Formal Verification

The mathematical process of proving that a program, such as a smart contract, satisfies specified properties under all possible conditions. Formal verification provides the highest level of assurance for critical applications by eliminating entire classes of bugs through mathematical proof rather than testing.

Full Node

A network participant that independently verifies all blocks and transactions, maintains sufficient state to validate new transactions, and does not rely on third parties for information about the ledger state. Full nodes provide the highest level of security and sovereignty for blockchain network participants.

Hardware Security Module (HSM)

A tamper-resistant physical device used to securely generate, store, and use cryptographic keys. HSMs meeting standards such as FIPS 140-2 Level 3 provide hardware-based protection against key extraction and are recommended for critical services including Digital Public Infrastructure registries and treasury management.

Hash Pointer

A reference to off-chain content that includes a cryptographic hash of the data, enabling integrity verification without exposing the underlying information. Hash pointers allow blockchain systems to verify data existence and authenticity while storing actual data in external systems, supporting privacy and data minimization requirements.

Immutability

The property of blockchain data that prevents modification or deletion once recorded. Achieved through cryptographic linking of blocks and distributed consensus, immutability provides tamper-evidence and auditability. However, immutability creates tension with data protection rights such as the Right to Erasure, necessitating architectural patterns like off-chain storage and crypto-shredding.

Inter-Blockchain Communication (IBC)

A protocol for secure, authenticated communication between different blockchain networks, enabling cross-chain transfers of tokens and data without centralized intermediaries. IBC provides a structured interoperability model based on light client verification and trusted relayer operations.

Interoperability

The ability of different systems to exchange and use information effectively. In the context of Digital Public Infrastructure, interoperability encompasses technological compatibility (technical protocols and APIs), semantic alignment (common data models and meanings), legal harmonization (compatible regulatory frameworks), and organizational coordination (governance arrangements between participating entities).

Issuer-Holder-Verifier Model

A credential interaction pattern where an issuer signs and issues a credential, a holder stores and presents the credential, and a verifier checks the cryptographic proof and credential status. This model maps to agency roles and accountability in Digital Public Infrastructure contexts and enables privacy-preserving credential verification.

Layer 2 (L2)

A protocol that processes transactions off the base blockchain layer (Layer 1) while inheriting security properties from it. Layer 2 solutions, including rollups and payment channels, improve scalability and reduce costs while maintaining connection to the underlying blockchain's security guarantees.

Light Client

A network client that verifies blockchain data using block headers and Merkle proofs without downloading and storing the full blockchain state. Light clients enable resource-constrained devices to participate in blockchain verification while minimizing bandwidth and storage requirements.

Merkle Proof

A cryptographic proof demonstrating that a specific piece of data is included in a Merkle tree, using only a small subset of the tree's nodes. Merkle proofs enable efficient verification of data inclusion without requiring access to the complete dataset, supporting auditability while minimizing data retrieval.

Merkle Tree

A hierarchical data structure where each leaf node contains a hash of a data block, and each non-leaf node contains a hash of its child nodes. Merkle trees enable efficient verification of data integrity and inclusion without downloading entire datasets, forming the basis for lightweight blockchain verification.

Multi-Party Computation (MPC)

Cryptographic techniques enabling multiple parties to jointly compute a function over their private inputs without revealing those inputs to each other. MPC enables distributed key generation and signing for critical operations, eliminating single points of compromise and enhancing security for custody and governance applications.

Multisignature (Multisig)

A cryptographic scheme requiring multiple private keys to authorize a transaction or operation. Multisig arrangements are used for governance, treasury management, and high-value operations where no single party should have unilateral control.

Off-Chain Storage

Data stored outside the blockchain in external systems such as databases, secure data vaults, or decentralized storage networks, with on-chain references or proofs enabling verification. Off-chain storage patterns enable privacy compliance, data correction, and erasure workflows while maintaining on-chain integrity anchors.

On-Chain Governance

Governance processes conducted through blockchain transactions, typically involving token-based voting and execution through smart contracts. On-chain governance provides transparency and accountability for protocol changes, parameter updates, and collective decision-making.

Oracle

A mechanism for providing off-chain data to smart contracts, such as price feeds, event outcomes, or sensor readings, often with cryptographic or economic assurances of data integrity. Oracles are critical components for blockchain applications that interact with real-world information and require careful governance and security considerations.

Permissioned Network

A blockchain network where validators and/or participants require authorization to join and operate. Permissioned networks are typical for enterprise and government deployments where accountability, compliance, and controlled access are required. Participation is restricted to known, vetted entities.

Permissionless Network

A blockchain network where any party can participate in consensus, submit transactions, and operate nodes without requiring authorization. Permissionless networks prioritize censorship resistance and open access but may present challenges for regulatory compliance and accountability.

Privacy by Design

An approach to system development that embeds privacy protections into the technical architecture from the outset, rather than adding them as an afterthought. For blockchain implementations, this includes avoiding direct on-chain storage of personal data, implementing pseudonymization, and enabling data subject rights through cryptographic techniques.

Proof of Authority (PoA)

A consensus mechanism where a pre-selected set of authorized validators produce blocks based on their identity and reputation. PoA provides high throughput and energy efficiency, making it suitable for permissioned consortium networks where validators are known and accountable entities.

Proof of Stake (PoS)

A consensus mechanism where validators are selected to produce blocks based on the amount of cryptocurrency they have staked as collateral. Validators who act maliciously risk losing their stake through slashing penalties. PoS provides security through economic incentives rather than computational work.

Rollup

A Layer 2 scaling solution that executes transactions off-chain but posts transaction data or proofs to the base layer blockchain. Rollups inherit the security of the underlying blockchain while achieving higher throughput. Optimistic rollups assume validity unless challenged, while zero-knowledge rollup (ZK rollups) provide cryptographic proofs of correct execution.

Selective Disclosure

The ability for a credential holder to reveal only specific attributes from a credential rather than the entire credential content. Selective disclosure supports data minimization principles by enabling verification of necessary claims without exposing additional personal information.

Self-Sovereign Identity (SSI)

An identity model where individuals control their own digital identifiers and credentials without relying on centralized authorities. SSI empowers users as owners of their identity data, aligning with data protection principles of user control and consent.

Smart Contract

Computer code deployed on a blockchain that executes automatically when predefined conditions are met. Smart contracts enable programmable, self-executing agreements and are fundamental to blockchain applications. Key policy considerations include upgradability governance, security auditing requirements, and formal verification for critical applications.

Stablecoin

A cryptographic token designed to maintain a stable value relative to a reference asset, typically a fiat currency, through mechanisms such as asset reserves or algorithmic supply management. Stablecoins raise policy considerations around reserve transparency, consumer protection, systemic risk, and monetary policy implications.

Token

A digital representation of value, rights, or assets on a blockchain. Tokens may be fungible (interchangeable, like currency) or non-fungible (unique, representing specific assets). Depending on their characteristics, tokens may be subject to various regulatory classifications.

Transaction

A signed instruction that changes blockchain state, such as a token transfer or smart contract invocation. Transactions include sender and recipient information, the operation to be performed, and a cryptographic signature proving authorization.

Trust Framework

A comprehensive policy and technical framework defining assurance levels, roles, accreditation requirements, audit procedures, and dispute resolution mechanisms for digital trust services. Trust frameworks are essential for deploying Decentralized Identifiers and Verifiable Credentials at scale.

Validator

A network participant authorized to participate in consensus by proposing or attesting to blocks. Validators are responsible for verifying transactions and maintaining the integrity of the blockchain. In permissioned networks, validators are typically known entities that have been vetted and authorized by network governance.

Verifiable Credential (VC)

A tamper-evident credential format signed by an issuer, designed for selective disclosure and cryptographic verification. Verifiable Credentials enable privacy-preserving credentialing with data minimization, supporting offline verification and cross-system interoperability according to the W3C VC data model.

Verifiable Presentation (VP)

A holder-generated presentation of one or more Verifiable Credentials, often including selective disclosure proofs. Verifiable Presentations minimize data sharing by allowing holders to prove specific claims without revealing complete credential contents.

Virtual Asset Service Provider (VASP)

A regulated entity that conducts exchange, transfer, custody, issuance, or related services for virtual assets. VASPs represent a key regulatory perimeter for licensing, Anti-Money Laundering and Counter-Terrorism Financing compliance, consumer protection, and cybersecurity obligations.

Zero-Knowledge Proof (ZKP)

A cryptographic proof that demonstrates a statement is true without revealing the underlying private information. ZKPs enable privacy-preserving compliance verification, allowing parties to prove attributes such as age, eligibility, or credential validity without exposing sensitive personal data. Common implementations include ZK-SNARKs and ZK-STARKs.

Zero-Trust Architecture

A security model that assumes no implicit trust, requiring authentication, authorization, and continuous evaluation for every access request regardless of network location or previous authentication status. Zero-trust principles are recommended for national-scale digital systems, including blockchain node operations and Digital Public Infrastructure integration endpoints.

CHAPTER 1: INTRODUCTION

1.1 Preamble

The Government of the People's Republic of Bangladesh, recognizing the transformative potential of Distributed Ledger Technology (DLT) and blockchain systems in advancing national development objectives, hereby promulgates this National Blockchain Policy. This Policy establishes a comprehensive framework for the responsible adoption, deployment, and governance of blockchain technology across public and private sectors, ensuring alignment with Bangladesh's constitutional principles, development aspirations, and regulatory architecture.

Blockchain technology, as a subset of Distributed Ledger Technology (DLT), represents a distributed data structure wherein transactions are grouped into cryptographically linked blocks, replicated across multiple nodes in a peer-to-peer network, and validated through consensus mechanisms without reliance on a single trusted third party. Each block contains a batch of transactions, a cryptographic hash of the previous block forming an immutable chain, a timestamp, and consensus-related metadata. The technology exhibits properties of immutability, transparency, data provenance, and distributed consensus that offer significant potential to enhance accountability, data integrity, and operational efficiency across diverse application domains.

The global architecture of public administration is undergoing a fundamental transformation. Governments worldwide are transitioning from the digitization of analog processes toward the creation of Digital Public Infrastructure (DPI) that is interoperable, scalable, and resilient. Within this paradigm, blockchain technology has graduated from speculative experimentation to becoming a critical layer of the sovereign technology stack. Nations such as India, China, Singapore, Estonia, and various jurisdictions in Latin America and Africa are deploying blockchain to address chronic challenges of trust, transparency, and efficiency in public service delivery.

This Policy builds upon the foundations laid by the National Blockchain Strategy: Bangladesh (2021), which articulated the vision of transforming Bangladesh into a blockchain-enabled nation. It incorporates learnings from global best practices while ensuring strict compliance with the National Data Governance Ordinance, 2025 (NDGO), the Personal Data Protection Ordinance, 2025 (PDPO), and the Cyber Safety Ordinance, 2025 (CSO). The Policy recognizes that Bangladesh stands at a unique vantage point, having enacted these three landmark ordinances simultaneously, creating an opportunity to build a Trust Infrastructure that is secure by design and rights-preserving by default.

1.2 Background and Context

1.2.1 Bangladesh's Digital Transformation Journey

Bangladesh stands at a pivotal juncture in its digital transformation journey. The nation has witnessed remarkable progress in digital adoption, with over 120 million internet users and a rapidly growing digital economy. However, the current landscape presents both significant opportunities and pressing challenges that necessitate advanced technological interventions.

The existing digital ecosystem faces challenges of fragmented data islands, wherein isolated registries for National Identity, taxation, land records, education, and health operate without real-time coordination. This fragmentation results in duplication of digital assets, increased operational costs, vulnerability to data breaches, and inability to deliver seamless end-to-end digital services. The absence of secure interoperability mechanisms between government agencies impedes efficient service delivery and creates friction for citizens navigating multiple bureaucratic touchpoints.

The Fourth Industrial Revolution (4IR) exposes both new challenges and exciting opportunities for nations worldwide. Blockchain technology is widely regarded as one of the core and foundational technologies driving this transformation. Only countries with expertise in these emerging technologies can successfully meet the challenges and exploit the opportunities presented by the digital age. Recognizing this imperative, the Government of Bangladesh has committed to exploring how blockchain technology can prepare the nation for future challenges and benefit its citizens in achieving the Sustainable Development Goals (SDGs) by 2030.

1.2.2 Legal and Regulatory Foundation

The enactment of three landmark ordinances in 2025 has established a robust legal architecture for data governance, privacy protection, and cybersecurity that forms the foundation for digital transformation for Bangladesh with AI and blockchain adoption as backbone:

The National Data Governance Ordinance, 2025 (NDGO) creates the National Data Governance Authority (NDGA) and establishes the Bangladesh National Digital Infrastructure Architecture (BNDIA) and the National Responsible Data Exchange (NRDEX) platform. The NDGO mandates interoperability across government systems, defines data classification frameworks, establishes Chief Data Officers at institutional levels, and creates enforcement mechanisms for data governance compliance. Section 21 legally establishes BNDIA as the architectural backbone for Bangladesh's Digital Public Infrastructure.

The Personal Data Protection Ordinance, 2025 (PDPO) fundamentally redefines the relationship between citizens and their data, declaring personal data as the owned property of data subjects. The PDPO grants fundamental rights including the Right to Access (Section 10), Right to Data Portability through Federated Interoperable Ecosystems (Section 11), Right to Correction and Erasure (Section 12), Right to Consent Withdrawal (Section 13), and mandates System-Wide Propagation of data updates across all systems (Section 14). These provisions create specific technical requirements that any blockchain implementation must address through appropriate architectural patterns.

The Cyber Safety Ordinance, 2025 (CSO) introduces the Critical Information Infrastructure (CII) designation and establishes the National Security Operations Center (NSOC) under the National Cybersecurity Agency (NCSA). The CSO defines CII as any infrastructure whose damage would impact public safety, economic security, or sovereignty. Blockchain systems supporting government functions will be designated as CII, subjecting them to heightened security standards, mandatory NSOC connectivity, regular security audits, and incident reporting requirements. The CSO provides a modern definition of Data-Store that explicitly encompasses blockchain ledgers, ensuring that legal provisions apply to decentralized networks.

These three ordinances work in concert to create a comprehensive legal architecture. The CSO establishes the security perimeter, the PDPO protects individual rights within that perimeter, and the NDGO enables productive and secure use of data across government and the private sector. Together, they align Bangladesh with international standards such as the European Union's General Data Protection Regulation (GDPR) while addressing the nation's unique socioeconomic context.

1.2.3 The National Digital Transformation Strategy

The National Digital Transformation Strategy articulates Bangladesh's comprehensive roadmap for digital evolution, anchored in nine core pillars: empowering citizens, creating efficient government, enabling businesses, building interoperable Digital Public Infrastructure, expanding connectivity, strengthening policy and governance, undertaking AI-driven workforce upskilling, establishing an independent data governance authority, and ensuring ethical AI deployment.

Central to this strategy is the phased interoperability roadmap progressing through three stages. The initial stage addresses the current fragmented state of data islands where isolated registries operate without real-time coordination. The intermediate stage establishes a secure hub-and-spoke model connecting priority ministries through the System Integration for Trusted Access (SITA) Gateway and standardized APIs. The final stage achieves full interoperability with AI-enabled analytics, unified identity management, and elimination of manual data exchange processes.

The strategy explicitly identifies blockchain as a critical enabling technology within the National Data Center Ecosystem. Stage 2 of the Digital Transformation Strategy introduces Blockchain Remote Procedure Call (RPC) capabilities as distributed ledger infrastructure enabling transparent, immutable record-keeping for critical government transactions. This technology supports applications ranging from land registration to educational credential verification, positioning blockchain as a foundational layer of the national digital infrastructure.

1.2.4 The Immutability Paradox: A Central Challenge

The most critical technical and legal challenge in Bangladesh's blockchain adoption is the tension between blockchain's inherent immutability and the data subject rights mandated by the PDPO. Standard blockchain architecture creates append-only ledgers where data, once written, cannot be altered or deleted without breaking the cryptographic chain. However, the PDPO declares personal data as the owned property of citizens and grants rights to erasure and consent withdrawal.

If a citizen revokes consent under PDPO provisions, a Data Fiduciary must erase their data. On an immutable blockchain ledger, such deletion is technically impossible in the traditional sense. This creates what has been termed the Immutability Paradox: the very properties that make blockchain valuable for trust and auditability conflict with fundamental data protection rights.

Unlike early blockchain adopters who are now retrofitting privacy protections into existing systems, Bangladesh has the opportunity to build its National Blockchain Framework with this paradox resolved from inception. This Policy mandates Privacy by Design architectures including off-chain data storage with on-chain hash pointers, crypto-shredding mechanisms for effective erasure, and pseudonymization techniques to prevent re-identification across transactions.

1.3 Purpose and Scope

1.3.1 Policy Objectives

This Policy establishes the governance framework, technical standards, regulatory mechanisms, and implementation roadmap for blockchain technology adoption in Bangladesh. The Policy aims to:

- Enable the Government of Bangladesh to harness blockchain technology for enhancing transparency, accountability, efficiency, and citizen trust in public service delivery while maintaining strict adherence to the legal and regulatory architecture established by the NDGO, PDPO, and CSO.
- Establish a sovereign, permissioned National Blockchain Infrastructure (NBI) that integrates with the BNDIA and NRDEX platforms, providing integrity anchoring, credential status verification, and audit trail capabilities for transactions processed through Digital Public Infrastructure.
- Provide clear guidance for government agencies, state-owned enterprises, private sector entities, academic institutions, and international development partners on the responsible adoption and deployment of blockchain technology within Bangladesh.
- Foster innovation and capacity building in blockchain technology while ensuring consumer protection, data privacy, cybersecurity, and regulatory compliance across all blockchain deployments.

1.3.2 Scope of Application

This Policy applies to the following entities and activities:

All government ministries, divisions, departments, directorates, and agencies deploying or utilizing blockchain-based systems for any purpose, including but not limited to record-keeping, verification, credential issuance, supply chain tracking, and inter-agency data exchange.

State-owned enterprises, autonomous bodies, statutory organizations, and public corporations implementing distributed ledger solutions for operational purposes or citizen-facing services.

Private sector entities providing blockchain services to government agencies, operating blockchain infrastructure within Bangladesh, or processing data classified under the NDGO framework through blockchain systems.

Academic institutions, research organizations, and think tanks conducting blockchain-related research and development, particularly those receiving government funding or collaborating with public sector entities.

International organizations, development partners, non-governmental organizations, and donor agencies supporting blockchain initiatives in Bangladesh or operating blockchain systems that process data of Bangladeshi citizens.

1.3.3 Matters Outside Scope

This Policy explicitly does not regulate the following matters, which remain under the jurisdiction of their respective regulatory authorities:

Cryptocurrency and Virtual Currency Regulation: Matters relating to cryptocurrency trading, virtual currency exchanges, crypto asset markets, and the legal status of cryptocurrencies as currency or legal tender remain exclusively under the jurisdiction of Bangladesh Bank pursuant to the Bangladesh Bank Order, 1972, the Foreign Exchange Regulation Act, 1947, the Anti-Money Laundering Act, 2012, and applicable monetary and financial services legislation. Any blockchain application involving payment instruments, money transmission, or financial services shall require Bangladesh Bank authorization.

Virtual Asset Service Providers (VASPs): The licensing, supervision, and regulation of Virtual Asset Service Providers conducting exchange, transfer, custody, issuance, or related services for virtual assets are governed by Bangladesh Bank's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) frameworks and applicable financial sector regulations.

Securities and Capital Markets: Tokenized securities, security token offerings, blockchain-based capital market instruments, and digital asset investment schemes are regulated by the Bangladesh Securities and Exchange Commission (BSEC) under the Securities and Exchange Ordinance, 1969, and related legislation. Decentralized finance (DeFi) protocols offering securities-like products fall within BSEC jurisdiction.

Central Bank Digital Currency (CBDC): The development, issuance, and regulation of any Central Bank Digital Currency representing sovereign currency issued by Bangladesh Bank remains exclusively within Bangladesh Bank's monetary policy authority.

Cross-Border Remittance Services: Blockchain-based remittance services, cross-border payment systems, and international money transfer services require authorization from Bangladesh Bank and compliance with foreign exchange regulations.

Trade and Commerce: Trade-related aspects of digital assets, cross-border e-commerce involving blockchain verification, and consumer protection in blockchain-enabled commerce fall under the jurisdiction of the Ministry of Commerce pursuant to applicable trade and commerce legislation.

Entities operating in these domains shall comply with the regulations, circulars, guidelines, and directives issued by the respective regulatory authorities. This Policy shall apply to the underlying blockchain technology infrastructure and technical standards where such infrastructure intersects with Digital Public Infrastructure under NDGA oversight.

CHAPTER 2: VISION, MISSION AND STRATEGIC OBJECTIVES

2.1 Vision Statement

To transform Bangladesh into a blockchain-enabled nation where Distributed Ledger Technology serves as a trusted infrastructure layer for Digital Public Infrastructure, enhancing government transparency, citizen empowerment, economic efficiency, and national competitiveness while maintaining strict adherence to data protection, privacy rights, cybersecurity imperatives, and the principles of data sovereignty.

This vision recognizes blockchain not as an end in itself but as a powerful enabling technology that, when appropriately deployed within the national digital architecture, can automate trust, guarantee privacy by design, and preserve sovereignty over critical national data assets. The vision aligns with the broader aspirations of digital transformation strategy to establish Bangladesh as a developed nation with a knowledge-based economy powered by advanced digital infrastructure.

2.2 Mission Statement

To establish a sovereign, permissioned blockchain ecosystem that integrates seamlessly with the Bangladesh National Digital Infrastructure Architecture (BNDIA) and the National Responsible Data Exchange (NRDEX), enabling secure and verifiable data sharing across government agencies while protecting citizen rights, fostering innovation in the digital economy, and positioning Bangladesh as a regional leader in blockchain-enabled governance.

The mission encompasses building technical infrastructure, establishing governance frameworks, developing human capacity, creating enabling regulations, and fostering an ecosystem where government, private sector, academia, and civil society can collaborate to realize the transformative potential of blockchain technology for national development.

2.3 Strategic Objectives

2.3.1 Infrastructure Development Objectives

Objective 1: Establish a National Blockchain Infrastructure (NBI) as a sovereign permissioned consortium network operated by designated government entities under the oversight of the National Data Governance Authority (NDGA). The NBI shall be hosted within the National Data Center Ecosystem comprising the National Data Center (NDC), Disaster Recovery facilities, Bangladesh Data Centre Company Limited (BDCCL), and accredited private data centers, ensuring complete data sovereignty and localization compliance.

Objective 2: Integrate the National Blockchain Infrastructure with the BNDIA framework and NRDEX platform, positioning NRDEX as the authoritative Oracle providing authenticated off-chain data from government sources to on-chain smart contracts. This integration shall enable blockchain to function as a ledger of events and integrity layer for transactions passing through Digital Public Infrastructure.

Objective 3: Deploy Blockchain Remote Procedure Call (RPC) capabilities within the National Data Center Ecosystem as specified in Stage 2 of the Digital Transformation Strategy, enabling distributed ledger infrastructure for transparent, immutable record-keeping of critical government transactions including land registration, educational credential verification, and public procurement.

2.3.2 Privacy and Compliance Objectives

Objective 4: Ensure full compliance with the Personal Data Protection Ordinance, 2025 through mandatory adoption of privacy-preserving architectures. All blockchain implementations processing personal data shall utilize off-chain data storage patterns where personal data resides in secured data vaults connected via NRDEX, with only cryptographic hash pointers recorded on-chain for integrity verification.

Objective 5: Implement crypto-shredding mechanisms across all blockchain systems processing personal data, enabling effective satisfaction of the Right to Erasure under PDPO Section 12 through secure deletion of encryption keys, rendering on-chain hash references mathematically unusable without breaking blockchain integrity.

Objective 6: Deploy pseudonymization techniques including rotating Decentralized Identifiers (DIDs) to prevent profiling of citizens across transactions, ensuring that blockchain implementations do not create persistent trails enabling unauthorized tracking or surveillance of individual activities.

2.3.3 Security and Critical Infrastructure Objectives

Objective 7: Integrate blockchain systems with the Critical Information Infrastructure (CII) protection framework under the Cyber Safety Ordinance, 2025. All National Blockchain Infrastructure components and blockchain systems processing government data shall be designated as CII, with mandatory connectivity to the National Security Operations Center (NSOC) for real-time security monitoring.

Objective 8: Ensure robust security controls across all blockchain deployments including Hardware Security Module (HSM) integration for cryptographic key management, Multi-Party Computation (MPC) for distributed key operations, Security Information and Event Management (SIEM) integration, and Endpoint Detection and Response (EDR) capabilities on node infrastructure.

Objective 9: Establish incident response capabilities coordinated with the National Cyber Emergency Response Team (NCERT), with defined incident reporting timelines, response playbooks, and regular penetration testing and vulnerability assessments for all blockchain infrastructure.

2.3.4 Capacity Building and Innovation Objectives

Objective 10: Develop national capacity in blockchain technology through education, training, research, and industry development programs aligned with the Bangladesh Computer Council (BCC).

Objective 11: Integrate blockchain curriculum into universities and polytechnic institutions, establish professional certification programs, and create pathways for international collaboration with leading blockchain research institutions and standards bodies.

Objective 12: Establish a regulatory sandbox for controlled experimentation with innovative blockchain applications, providing time-limited authorizations for experimental deployments with close monitoring and clear graduation pathways to full authorization.

2.3.5 Application Domain Objectives

Objective 13: Implement blockchain-based solutions across priority application domains including digital identity and credential verification, land records and property registration, public finance and procurement, supply chain management for agriculture and pharmaceuticals, educational certificate verification, and health data exchange.

Objective 14: Deploy Self-Sovereign Identity (SSI) capabilities enabling citizens to hold Verifiable Credentials for education, professional licenses, health records, and property ownership in citizen-controlled digital wallets, empowering them as owners of their data consistent with PDPO principles.

2.3.6 Interoperability and Standards Objectives

Objective 15: Promote interoperability through adoption of open standards including W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), ISO/TC 307 blockchain standards, ISO 20022 financial messaging standards for payment interoperability, and Inter-Blockchain Communication (IBC) protocols for cross-chain messaging.

Objective 16: Establish technical bridges enabling interoperability between Bangladesh's National Blockchain Infrastructure and international blockchain networks for trade facilitation, particularly for Ready-Made Garment sector export documentation and Letters of Credit, following models such as Singapore's TradeTrust framework.

Objective 17: Foster a regulatory environment that enables responsible innovation while protecting consumers, maintaining financial stability, preventing illicit activities, and ensuring that blockchain technology serves the broader public interest.

CHAPTER 3: GUIDING PRINCIPLES

The deployment and governance of blockchain technology in Bangladesh shall be guided by the following foundational principles, which ensure alignment with constitutional values, statutory requirements, and international best practices. These principles provide the normative framework within which all blockchain initiatives must operate.

3.1 Data Sovereignty and Localization

The principle of data sovereignty mandates that Bangladesh maintains ultimate control over data generated within its territory and concerning its citizens. Blockchain systems processing government data or citizen information shall respect this sovereignty through strict adherence to data localization requirements.

3.1.1 Infrastructure Localization Requirements

All blockchain systems processing data classified as Restricted or Confidential under the NDGO data classification framework shall operate exclusively on infrastructure located within the sovereign territory of Bangladesh. Validator nodes for government blockchain networks shall be physically hosted in data centers within Bangladesh's territorial boundaries, including the National Data Center at Kaliakair, disaster recovery facilities, BDCCL facilities, and NDGA-accredited private data centers.

Node operators for government blockchain networks shall be domestically registered entities subject to Bangladeshi jurisdiction. Foreign entities may participate in consortium arrangements only where they maintain registered presence within Bangladesh, submit to local regulatory oversight, and ensure that all data processing occurs within Bangladesh's territory.

3.1.2 Cross-Border Data Transfer Controls

Cross-border data transfers via blockchain systems shall comply with Sections 29-30 of the PDPO and Section 43 of the NDGO regarding adequate protection levels and NDGA authorization. Blockchain networks with international nodes shall be designed such that data classified as Restricted or Confidential is not replicated to nodes outside Bangladesh.

For blockchain applications requiring international interoperability, such as trade finance and supply chain verification, only non-sensitive transaction metadata and cryptographic proofs shall be shared across borders. Anchoring non-sensitive hashes to public chains for international verification is permitted. Actual citizen data and government records shall remain within domestic infrastructure, with international parties able to verify authenticity through cryptographic mechanisms without accessing underlying data.

The NDGO's requirement for strict controls over restricted data, which affects national security or critical infrastructure, effectively prohibits the use of public, permissionless blockchains where data is replicated on global nodes for core government functions. Permissionless networks may only be used for integrity anchoring where no actual data, only cryptographic hashes, crosses national boundaries.

3.2 Privacy by Design

Privacy by Design is a fundamental principle requiring that privacy protections be embedded into the technical architecture of blockchain systems from the design phase, rather than being added as afterthought controls. This principle is essential for reconciling blockchain's immutability with the data subject rights guaranteed under the PDPO.

3.2.1 Prohibition on Direct On-Chain Personal Data Storage

Personal data, as defined in Section 2(18) of the PDPO, shall not be stored directly on-chain in any blockchain system operating within the scope of this Policy. The immutable nature of blockchain ledgers creates a direct conflict with the Right to Erasure under PDPO Section 12. Storing personal data on an append-only ledger would permanently violate a citizen's right to have their data erased upon consent withdrawal.

Instead, all blockchain implementations shall utilize off-chain storage patterns where personal data resides in secured, encrypted data vaults operated by authorized Data Fiduciaries. These vaults shall be connected to the National Responsible Data Exchange (NRDEX) for governed access. Only cryptographic hash pointers, computed using approved hash functions such as SHA-256 or SHA-3, shall be recorded on the blockchain. These hashes serve as fingerprints enabling verification of data existence and integrity without exposing content.

3.2.2 Crypto-Shredding for Effective Erasure

When a citizen exercises the Right to Erasure under PDPO Section 12 or withdraws consent under Section 13, the Data Fiduciary shall implement crypto-shredding by securely deleting the encryption key used to access the off-chain data, or by deleting the off-chain record itself from all storage locations.

Upon crypto-shredding, the hash pointer remaining on the blockchain becomes a reference to mathematically inaccessible data. The hash cannot be reversed to reveal the original data, and without the encryption key, the off-chain encrypted data cannot be decrypted. This renders the hash functionally equivalent to deleted data, thereby satisfying the erasure requirement without breaking the blockchain's cryptographic chain.

All blockchain systems shall maintain crypto-shredding capabilities with documented procedures, audit trails of erasure requests and completions, and technical verification mechanisms confirming that erasure has been effectively implemented across all relevant systems including backup systems.

3.2.3 Pseudonymization and Rotating Identifiers

While the PDPO recognizes pseudonymized data as compliant when keys are kept separate, blockchain addresses and public keys are inherently pseudonymous but potentially linkable. Sophisticated analytics and chain analysis techniques can potentially re-identify users by correlating transaction patterns.

To prevent unauthorized profiling across transactions, blockchain implementations shall mandate the use of rotating Decentralized Identifiers (DIDs). Each significant transaction context shall utilize a fresh DID, preventing the creation of comprehensive activity profiles tied to persistent identifiers. This technique, aligned with approaches used in the European Union's Digital Identity Wallet, ensures that blockchain's transparency benefits do not compromise citizen privacy.

3.3 Interoperability

Blockchain systems shall be designed for multi-dimensional interoperability as defined in Section 2 of the NDGO, encompassing technological, semantic, legal, and organizational dimensions. Isolated blockchain deployments that cannot communicate with the broader Digital Public Infrastructure shall not be approved for government use.

3.3.1 Technological Interoperability

All blockchain implementations shall interface with the Bangladesh National Digital Infrastructure Architecture (BNDIA) and the National Responsible Data Exchange (NRDEX) through standardized RESTful APIs with OpenAPI 3.0 specifications. API endpoints shall implement proper authentication using TRUST-CCA (Trust and Certificate Chain Authority) standards, authorization based on purpose limitation principles, and comprehensive audit logging.

Blockchain systems shall support standard data formats and messaging protocols including ISO 20022 for financial transactions and W3C data models for identity credentials. Inter-Blockchain Communication (IBC) protocols shall be implemented where different permissioned chains operated by various government agencies need to exchange authenticated messages and verify states across chain boundaries.

3.3.2 Semantic Interoperability

Blockchain systems shall adopt common data models, schemas, and metadata standards to ensure that information exchanged across systems carries consistent meaning. Interoperability profiles shall be developed for each application domain, defining the data elements, formats, and semantics required for consistent data exchange across government agencies and with authorized private sector participants.

All datasets and transactions on blockchain systems shall be tagged with consistent metadata per NDGA standards, enabling discovery, governance, and appropriate access control across the integrated digital ecosystem.

3.3.3 Legal and Organizational Interoperability

Legal interoperability requires alignment of regulatory frameworks governing blockchain operations across different agencies and jurisdictions. This Policy establishes the overarching legal framework; sector-specific guidance shall be developed in coordination with relevant regulators to address domain-specific requirements.

Organizational interoperability requires governance arrangements between participating entities including Data Resharing Agreements (DRAs) as specified under NDGO Section 23, service level agreements for node operations, incident response coordination mechanisms, and change management procedures for protocol upgrades affecting multiple agencies.

3.4 Zero-Trust Architecture

Consistent with the zero-trust architecture requirements defined in Section 2(16) of the NDGO, blockchain systems shall implement continuous verification of all access requests regardless of network location, identity, or prior authentication status. The traditional perimeter security model, which assumes trust for entities inside the network, is inadequate for distributed systems handling sensitive government data.

3.4.1 Continuous Authentication and Authorization

Every data access request, smart contract execution, transaction submission, and node operation shall be authenticated against verified identities and authorized against defined access policies. Authentication shall employ strong cryptographic mechanisms including digital signatures verified against trusted public key infrastructure.

Authorization decisions shall be made based on the principle of least privilege, granting only the minimal permissions required to perform specific tasks. Role-Based Access Control (RBAC) policies shall define what actions different categories of users and systems may perform, with all authorization decisions logged for audit purposes.

3.4.2 Micro-Segmentation and Network Controls

Blockchain infrastructure shall implement network micro-segmentation, isolating different components and limiting lateral movement in the event of compromise. Validator nodes, API gateways, key management systems, and administrative interfaces shall operate in separate network segments with controlled inter-segment communication.

All network communications between blockchain components shall be encrypted using Transport Layer Security (TLS) 1.3 or higher. Peer-to-peer communications between nodes shall use authenticated encrypted channels preventing eavesdropping and man-in-the-middle attacks.

3.4.3 Comprehensive Audit Logging

All authentication attempts, authorization decisions, data access events, smart contract executions, and administrative actions shall be logged with sufficient detail to reconstruct activities for audit and forensic purposes. Logs shall be protected against tampering, stored in accordance with retention requirements, and made available to authorized auditors and the NSOC as required.

3.5 Transparency and Accountability

Blockchain deployments shall maintain comprehensive transparency enabling verification of system operations while respecting privacy constraints. Accountability mechanisms shall ensure that all participants in blockchain ecosystems can be held responsible for their actions.

3.5.1 Transaction and Execution Transparency

All transactions processed through government blockchain systems shall maintain comprehensive audit trails enabling verification of transaction origin, authorization, content hashes, timestamp, and execution results. Smart contract executions shall be logged with inputs, outputs, and state changes, enabling independent verification of correct operation.

Blockchain explorers and query interfaces shall be provided to authorized users enabling them to verify transaction histories and confirm system operations. Citizens shall have access to view transactions affecting their records, consistent with the Right to Access under PDPO Section 10.

3.5.2 Governance Transparency

Validator set composition, consensus parameters, protocol versions, and upgrade governance decisions shall be documented and publicly available. Changes to network governance, including validator additions or removals, consensus parameter modifications, and smart contract upgrades, shall follow documented procedures with advance notice to stakeholders.

On-chain governance mechanisms, where implemented, shall provide transparent records of proposals, voting, and execution. Off-chain governance decisions affecting the network shall be documented in accessible governance records.

3.5.3 Regulatory Oversight

Blockchain systems shall provide regulatory access enabling designated oversight authorities including the NDGA, NCSA, and relevant sectoral regulators to monitor compliance with applicable requirements. This includes access to network telemetry, transaction records, smart contract code, and audit logs as required for regulatory purposes.

3.6 Technology Neutrality

This Policy adopts a technology-neutral approach to Distributed Ledger Technology, permitting the use of various blockchain platforms, consensus mechanisms, smart contract languages, and cryptographic implementations provided they meet the security, privacy, interoperability, and governance requirements established herein.

Specific technology choices for government deployments shall be determined through technical evaluation processes overseen by the National Blockchain Technical Committee (NBTC). Evaluations shall assess platforms against defined criteria including security posture, performance characteristics, energy efficiency, governance capabilities, ecosystem maturity, vendor independence, and alignment with national technical standards.

The Policy encourages adoption of open-source platforms where applicable to prevent vendor lock-in, enable independent security auditing, and ensure long-term sustainability and sovereignty over critical infrastructure. Proprietary platforms may be considered where they offer significant advantages and provide adequate contractual protections and source code escrow arrangements.

3.7 Inclusivity and Accessibility

Blockchain-based services shall be designed for universal accessibility, ensuring that all citizens can benefit from blockchain-enabled services regardless of technical literacy, disability status, geographic location, or socioeconomic circumstances.

User interfaces for citizen-facing blockchain services shall comply with Web Content Accessibility Guidelines (WCAG) 2.1 Level AA or higher, ensuring accessibility for persons with disabilities. Interfaces shall be available in Bengali and English, with consideration for additional languages where significant user populations exist.

Service design shall account for users with limited digital literacy through intuitive interfaces, clear guidance, and support channels. Alternative access mechanisms shall be provided for users who cannot directly interact with digital systems, ensuring that blockchain-enabled services do not create new barriers to access.

3.8 Sustainability

Blockchain consensus mechanisms shall be evaluated for energy efficiency and environmental impact as part of technical assessments. Energy-intensive consensus mechanisms such as Proof of

Work, which requires significant computational resources for mining, shall not be approved for government deployments.

Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), and other energy-efficient consensus protocols shall be preferred for permissioned government networks. These mechanisms provide adequate security and performance while minimizing environmental footprint.

The sustainability assessment shall also consider the long-term viability of chosen technologies, including platform maintenance commitments, community support, upgrade pathways, and alignment with evolving industry standards.

3.9 Security by Default

All blockchain systems shall implement security by default, wherein the most secure configuration is the default setting and users must explicitly opt into less secure options where legitimate use cases require flexibility. This principle ensures that security is not dependent on user knowledge or initiative.

Default security configurations shall include encrypted storage for all sensitive data, encrypted communications for all network traffic, multi-factor authentication for administrative access, hardware security module integration for key management, and comprehensive logging of security-relevant events.

CHAPTER 4: REGULATORY FRAMEWORK AND GOVERNANCE STRUCTURE

This chapter establishes the regulatory architecture, institutional arrangements, and governance mechanisms for blockchain technology in Bangladesh. The framework ensures appropriate oversight while enabling innovation, with clear delineation of responsibilities among regulatory authorities.

4.1 Regulatory Authority Structure

The governance of blockchain technology in Bangladesh operates within a multi-layered regulatory framework, with different authorities exercising jurisdiction over distinct aspects of blockchain deployment and operation.

4.1.1 National Data Governance Authority (NDGA)

The National Data Governance Authority, established under Section 9 of the NDGO as an independent statutory body with perpetual succession, shall serve as the primary regulatory authority for blockchain systems deployed within Digital Public Infrastructure. The NDGA operates under the oversight of the National Data Governance Policy Board chaired by the Chief Adviser.

The NDGA shall exercise the following functions with respect to blockchain governance pursuant to its mandate under NDGO Section 23:

Platform Approval: Evaluate and approve blockchain platforms, consensus mechanisms, and technology stacks for government use, ensuring alignment with BNDIA requirements and national technical standards.

Node Operator Designation: Designate and authorize validator node operators for the National Blockchain Infrastructure, establishing eligibility criteria, operational requirements, and ongoing compliance obligations.

Data Classification Oversight: Ensure that data stored on or referenced by blockchain systems is classified according to the four-tier framework (Public, Internal, Confidential, Restricted) established under NDGO Section 31, with appropriate controls implemented based on classification.

Compliance Monitoring: Monitor compliance with NDGO and PDPO requirements across all blockchain deployments, including data localization, privacy-preserving architectures, and interoperability standards.

NCSA Coordination: Coordinate with the National Cybersecurity Agency on Critical Information Infrastructure designations for blockchain systems, security standards, and incident response.

Technical Guidelines: Issue technical guidelines, standards, and reference architectures for blockchain implementations, updated periodically to reflect technological evolution and lessons learned.

The NDGA's six specialized divisions shall support blockchain governance: the Data Protection and Management Division for privacy compliance, the Technical Standards and Interoperability Division for API certification and NRDEX operations, the Legal and Compliance Division for enforcement, and the Citizen Data and AI Governance Division for identity-related blockchain applications.

4.1.2 National Blockchain Technical Committee (NBTC)

A National Blockchain Technical Committee (NBTC) shall be established under the NDGA to provide specialized technical expertise for blockchain governance. The NBTC shall comprise:

- Representatives from the ICT Division providing policy direction and coordination with national ICT strategy.
- Technical experts from the Bangladesh Computer Council and the Bangladesh Blockchain Centre of Excellence bringing deep technical expertise in blockchain technologies.
- Representatives from relevant line ministries including Finance, Land, Education, Health, and Commerce whose domains are priority areas for blockchain deployment.
- Academic representatives from leading universities with blockchain research programs, ensuring incorporation of latest research findings.
- Industry stakeholders representing blockchain service providers, technology companies, and professional associations, bringing practical implementation experience.

The NBTC shall discharge the following responsibilities:

- Conduct technical evaluations of blockchain platforms proposed for government adoption, assessing security, performance, scalability, governance, and compliance characteristics against defined criteria.
- Develop and maintain technical specifications, reference architectures, and implementation guides for the National Blockchain Infrastructure and sector-specific applications.
- Review and recommend updates to national blockchain standards in response to technological developments, security threats, and implementation experience.
- Advise on smart contract audit requirements, establish criteria for approved auditors, and maintain a registry of certified smart contract auditors.
- Coordinate research and development initiatives, identify emerging technologies for potential adoption, and liaise with international standards bodies including ISO/TC 307 and W3C.

4.1.3 National Cybersecurity Agency (NCSA)

The National Cybersecurity Agency, established under the Cyber Safety Ordinance, 2025, shall exercise cybersecurity oversight over all blockchain systems operating within the scope of this Policy. The NCSA's mandate encompasses:

Critical Information Infrastructure Designation: Blockchain infrastructure supporting government functions, including the National Blockchain Infrastructure and agency-specific blockchain systems processing classified data, shall be designated as Critical Information Infrastructure pursuant to CSO Section 2(6). This designation subjects operators to enhanced security requirements.

NSOC Integration: CII-designated blockchain systems shall establish real-time monitoring connections with the National Security Operations Center (NSOC), providing telemetry data enabling NSOC to detect anomalies, potential attacks, and security incidents affecting blockchain infrastructure.

Security Standards Enforcement: The NCSA shall specify security standards for blockchain systems, potentially requiring ISO 27001 certification for node operators, penetration testing schedules, vulnerability disclosure procedures, and security architecture reviews.

Audit and Assessment: The NCSA shall conduct or commission regular security audits of CII-designated blockchain systems, including smart contract security assessments, consensus mechanism evaluation, and infrastructure penetration testing.

Incident Response Coordination: Security incidents affecting blockchain systems shall be reported to the National Cyber Emergency Response Team (NCERT) within timelines prescribed by the NCSA. The NCERT shall coordinate incident response, forensic investigation, and recovery operations.

Security Information and Event Management: Blockchain operators shall implement SIEM systems providing real-time collection, analysis, and correlation of security events, with feeds to NSOC as required for national-level threat awareness.

4.1.4 Sectoral Regulators

Blockchain applications within specific sectors shall additionally be subject to oversight by relevant sectoral regulators, whose existing mandates apply to blockchain-based implementations of regulated activities:

Bangladesh Bank: Retains exclusive authority over matters relating to monetary policy, currency, foreign exchange, payment systems, banking regulation, and financial stability. Any blockchain application involving payment instruments, stored value, money transmission, inter-bank settlement, trade finance, or financial services shall require Bangladesh Bank authorization and comply with applicable regulations including:

Anti-Money Laundering Act, 2012 and associated regulations requiring customer due diligence, transaction monitoring, and suspicious activity reporting.

Foreign Exchange Regulation Act, 1947 for blockchain applications involving cross-border value transfer or foreign exchange transactions.

Payment and Settlement Systems Regulations for blockchain-based payment rails or settlement mechanisms.

Guidelines on Virtual Asset Service Providers, if promulgated, for entities conducting exchange, transfer, or custody services for virtual assets.

Bangladesh Securities and Exchange Commission (BSEC): Exercises jurisdiction over securities markets and investor protection. BSEC oversight applies to:

Tokenized securities representing equity, debt, or other investment instruments.

Security token offerings seeking to raise capital from investors.

Blockchain-based capital market infrastructure including trading, clearing, and settlement systems.

Digital asset investment schemes that may constitute collective investment schemes.

Decentralized finance protocols offering securities-like products to Bangladesh residents.

Ministry of Land: Shall oversee blockchain applications for land records, mutation, registration, and property rights verification. Blockchain implementations in this domain shall integrate with existing land administration systems and comply with the Registration Act, 1908, the Transfer of Property Act, 1882, and related legislation.

Ministry of Health and Family Welfare: Shall regulate blockchain systems processing health data, ensuring compliance with sensitive personal data requirements under PDPO Section 6. Health data blockchain systems shall implement additional safeguards including enhanced consent mechanisms, restricted access controls, and audit requirements appropriate to health information sensitivity.

Ministry of Commerce: Retains authority over trade-related aspects of blockchain applications including supply chain traceability for exports, certificates of origin, trade documentation, and consumer protection in blockchain-enabled commerce.

Ministry of Education and University Grants Commission: Shall oversee blockchain implementations for educational credential verification, ensuring alignment with academic standards and credential recognition frameworks.

4.2 Alignment with Existing Legal Framework

Blockchain implementations shall operate within the comprehensive legal framework established by the NDGO, PDPO, and CSO. This section details specific compliance requirements.

4.2.1 National Data Governance Ordinance, 2025 Compliance

Data Classification (NDGO Section 31): Data stored on or referenced by blockchain systems shall be classified according to the four-tier framework. Restricted data affecting national security or critical infrastructure, and confidential data, shall not be stored directly on-chain and shall be subject to the strictest controls including domestic-only node operation.

Interoperability Requirements (NDGO Section 13): Blockchain systems shall integrate with NRDEX and BNDIA using prescribed APIs and data exchange protocols. The NDGO's requirement for system-wide propagation of data updates aligns with blockchain's state synchronization capabilities, provided blockchain is integrated with NRDEX APIs.

Data Stewardship (NDGO Section 34): Each ministry deploying blockchain shall designate a Chief Data Officer responsible for data inventory, interoperability compliance, and coordination with NDGA. The CDO shall ensure blockchain deployments comply with ordinance provisions and BNDIA guidelines.

Purpose-Based Access (NDGO Section 14): Smart contracts implementing data access shall enforce purpose limitation and need-to-know principles. Access to data through blockchain systems shall be authorized only for specified, legitimate purposes.

Organizational Responsibilities (NDGO Section 34): Organizations deploying blockchain shall comply with technology infrastructure modernization requirements including zero-trust architecture, cloud-first policies, API-based integration, and open-source platform adoption where applicable.

4.2.2 Personal Data Protection Ordinance, 2025 Compliance

The PDPO establishes personal data as the owned property of data subjects and grants fundamental rights that create specific architectural requirements for blockchain implementations:

Consent Management (PDPO Section 5): Smart contracts processing personal data shall implement consent verification mechanisms integrated with authorized consent management platforms. No personal data processing shall occur without valid, verifiable consent.

Right to Access (PDPO Section 10): Blockchain systems shall provide mechanisms enabling data subjects to access their personal data. This includes query interfaces showing what data references exist on-chain and access to associated off-chain data.

Right to Data Portability (PDPO Section 11): Data subjects shall be able to receive their personal data in structured, commonly used formats and transfer to other Data Fiduciaries through

Federated Interoperable Ecosystems. Blockchain credential systems shall support standard formats enabling portability.

Right to Erasure (PDPO Section 12): Compliance shall be achieved through mandatory off-chain storage of personal data with only hash pointers on-chain, and crypto-shredding mechanisms enabling effective erasure through encryption key deletion.

System-Wide Propagation (PDPO Section 14): Blockchain implementations shall support system-wide propagation of data corrections through registry smart contracts that maintain pointers to the latest valid data state. When data is corrected in primary sources, the blockchain registry shall be updated to reflect the current state.

Sensitive Personal Data (PDPO Section 6): Biometric data, health data, genetic data, sexual orientation information, financial data, and children's data shall receive enhanced protection with mandatory encryption, restricted access controls, and additional consent requirements.

Cross-Border Transfer (PDPO Sections 29-30): Blockchain networks with international nodes or cross-border data flows shall comply with cross-border data transfer requirements including NDGA authorization, adequacy assessments of recipient jurisdictions, and appropriate safeguards.

4.2.3 Cyber Safety Ordinance, 2025 Compliance

CII Designation: National Blockchain Infrastructure and blockchain systems processing government data shall be designated as Critical Information Infrastructure, triggering enhanced security requirements and oversight.

NSOC Integration: CII-designated blockchain systems shall establish real-time monitoring connections with the National Security Operations Center, providing security telemetry and enabling coordinated threat response.

Incident Response: Security incidents affecting blockchain systems shall be reported to NCERT within timeframes prescribed by NCSA regulations. Operators shall maintain incident response capabilities coordinated with national frameworks.

Data-Store Definition: The CSO's definition of Data-Store explicitly encompasses blockchain ledgers and data used by AI agents and Large Language Models. Offenses related to unauthorized access, hacking, and data theft apply fully to decentralized networks, closing potential legal loopholes for Web3 crimes.

Criminal Liability: Unauthorized access to blockchain systems, smart contract manipulation, and other cyber offenses are punishable under CSO provisions. Section 46 specifies which offenses are bailable, non-bailable, or compoundable.

CHAPTER 5: TECHNICAL ARCHITECTURE AND STANDARDS

This chapter establishes the technical architecture, infrastructure requirements, and standards framework for blockchain implementations in Bangladesh. The architecture is designed to integrate with the Bangladesh National Digital Infrastructure Architecture (BNDIA) while ensuring compliance with the data governance, privacy, and security requirements established by the NDGO, PDPO, and CSO.

5.1 National Blockchain Infrastructure (NBI) Architecture

The National Blockchain Infrastructure (NBI) shall serve as the sovereign blockchain platform for government applications, providing a permissioned consortium network operated by designated government entities under NDGA oversight. The NBI architecture comprises multiple layers designed for modularity, scalability, and compliance with national requirements.

5.1.1 Infrastructure Layer

The NBI shall be hosted within the National Data Center Ecosystem to ensure complete data sovereignty and localization compliance. The infrastructure components include:

Primary Data Center: The National Data Center (NDC) at Kaliakair shall host the primary validator nodes and core network infrastructure. The NDC provides Tier III+ facilities with redundant power, cooling, and network connectivity meeting international standards for critical infrastructure.

Disaster Recovery Facility: A geographically separated Disaster Recovery (DR) site shall maintain synchronized replica nodes capable of assuming primary operations within defined Recovery Time Objectives (RTO) of four hours and Recovery Point Objectives (RPO) of fifteen minutes. The DR facility shall be located at minimum 200 kilometers from the primary data center.

BDCCL Integration: Bangladesh Data Centre Company Limited (BDCCL) facilities shall host additional validator nodes to ensure geographic distribution within Bangladesh and enhance network resilience. BDCCL nodes shall operate under the same governance and security requirements as NDC-hosted nodes.

Accredited Private Data Centers: Private data centers meeting NDGA accreditation standards may host NBI nodes for specific applications, subject to compliance verification, security audits, and governance agreements. Accreditation criteria shall include physical security, network infrastructure, personnel security clearances, and operational procedures.

5.1.2 Network Layer

The NBI network architecture shall implement the following components:

Validator Network: A permissioned set of validator nodes operated by designated government ministries, agencies, and accredited entities. The initial validator set shall include nodes operated by the ICT Division, National Board of Revenue, Ministry of Land, Ministry of Education, Ministry of Health, and Bangladesh Bank (for regulated financial applications). The validator set may be expanded through NDGA authorization following established governance procedures.

Full Node Network: Full nodes that independently verify all blocks and transactions, maintaining complete blockchain state. Government agencies requiring blockchain access shall operate full nodes to ensure sovereignty and reduce reliance on external RPC providers. Full nodes provide the highest level of security and data integrity assurance.

Archive Nodes: Specialized nodes maintaining complete historical state, enabling queries about past balances, contract storage, and transaction details at any block height. Archive nodes support regulatory supervision, audit requirements, and forensic investigations. At minimum, two archive nodes shall be maintained by the NDGA and NCSA respectively.

RPC Gateway Infrastructure: Blockchain Remote Procedure Call (RPC) endpoints providing authenticated API access to the NBI. RPC gateways shall implement rate limiting, access controls, and comprehensive logging. Public RPC endpoints for authorized applications and private RPC endpoints for internal government use shall be segregated.

Peer-to-Peer Networking: All inter-node communications shall use authenticated encrypted channels using Transport Layer Security (TLS) 1.3 or higher. Node discovery and peer management shall operate through permissioned mechanisms preventing unauthorized node participation.

5.1.3 Consensus Layer

The NBI shall employ consensus mechanisms appropriate for permissioned government networks, prioritizing deterministic finality, energy efficiency, and accountability.

Primary Consensus Mechanism: Practical Byzantine Fault Tolerance (PBFT) or PBFT-family protocols shall be the recommended consensus mechanism for NBI. PBFT provides deterministic finality, meaning transactions are irreversibly committed once confirmed without probabilistic rollback risk. The protocol tolerates up to f faulty or malicious nodes in a 3f+1 validator system while maintaining network integrity.

Alternative Mechanisms: Proof of Authority (PoA) may be employed for specific use cases where PBFT overhead is not justified. PoA provides high throughput and energy efficiency with identified validators bearing legal and organizational accountability. Proof of Stake (PoS) variants may be considered for applications requiring economic incentive alignment.

Prohibited Mechanisms: Proof of Work (PoW) consensus mechanisms requiring significant computational resources for mining shall not be approved for NBI or government blockchain deployments due to energy inefficiency and environmental impact concerns.

Consensus parameters including block time, validator rotation schedules, and quorum requirements shall be documented and subject to NBTC review. Changes to consensus parameters shall follow formal governance procedures with advance notice to network participants.

5.1.4 Execution Layer

The execution layer processes transactions and executes smart contract logic:

Smart Contract Runtime: The NBI shall support Ethereum Virtual Machine (EVM) compatible execution to leverage the extensive ecosystem of development tools, security auditing frameworks, and developer expertise. EVM compatibility enables use of established languages such as Solidity and Vyper while maintaining access to mature testing and verification tools.

Alternative Runtimes: WebAssembly (WASM) based runtimes may be supported for specific applications requiring performance optimization or language flexibility. Any alternative runtime shall undergo NBTC security evaluation before deployment.

Gas and Resource Management: Transaction processing costs on NBI shall be managed through resource allocation mechanisms rather than cryptocurrency-based gas fees. Government agencies shall receive resource allocations based on operational requirements, with usage monitored and reported for capacity planning.

5.1.5 Application Layer

The application layer comprises smart contracts and decentralized applications (DApps) deployed on NBI:

Registry Contracts: Core registry smart contracts shall maintain authoritative records for credential status (revocation registries), document hashes (integrity anchors), and DID resolution (identity registries). Registry contracts shall be deployed by authorized issuers and maintained under strict governance controls.

Credential Contracts: Smart contracts supporting the issuance, verification, and revocation of Verifiable Credentials. These contracts shall implement W3C VC data model standards and integrate with the national trust framework.

Integration Contracts: Oracle contracts providing authenticated connections between NBI and off-chain systems, particularly NRDEX. The NRDEX Oracle shall serve as the authoritative source for off-chain government data accessed by smart contracts.

5.2 Integration with Bangladesh National Digital Infrastructure Architecture

The NBI shall integrate seamlessly with BNDIA components to function as the integrity and trust layer within the national digital ecosystem.

5.2.1 NRDEX Integration

The National Responsible Data Exchange (NRDEX) serves as the central platform for secure, API-based cross-agency data sharing. NBI integration with NRDEX shall operate as follows:

NRDEX as Authoritative Oracle: NRDEX shall serve as the trusted oracle providing authenticated off-chain data to NBI smart contracts. When a smart contract requires verification of government records (such as identity confirmation, land ownership, or educational credentials), NRDEX provides cryptographically signed attestations that the contract can verify on-chain.

Hash Anchoring: Data records processed through NRDEX may be anchored to NBI by storing cryptographic hashes on-chain. This creates immutable proof of data existence and integrity at specific points in time without storing actual data on the blockchain.

Event Logging: Significant data exchange events processed through NRDEX may be logged to NBI for audit trail purposes. Events include credential issuances, data access grants, and consent records, providing transparent and tamper-evident audit capabilities.

API Standards: Integration between NBI and NRDEX shall use standardized RESTful APIs conforming to OpenAPI 3.0 specifications. API authentication shall use TRUST-CCA certificates ensuring mutual authentication between systems.

5.2.2 SITA Gateway Integration

The System Integration for Trusted Access (SITA) Gateway connects priority ministries during the STAR phase of digital transformation. NBI shall integrate with SITA to:

- Provide blockchain-based verification services accessible through SITA APIs, enabling ministries to verify document authenticity and credential status without direct NBI access.
- Log inter-ministry data exchanges for audit purposes where required by data sharing agreements.
- Support graduated blockchain adoption as ministries transition from SITA-mediated access to direct NBI integration.

5.2.3 Unified Identity Layer Integration

The NBI shall integrate with the Unified Identity Layer (oneID) to provide blockchain-enhanced identity services:

DID Registry: A national DID registry deployed on NBI shall enable resolution of Decentralized Identifiers to DID Documents containing public keys and service endpoints. The registry shall support the W3C DID Core specification with a Bangladesh-specific DID method (did:bd).

Credential Status Registry: An on-chain registry tracking the status (active, suspended, revoked) of Verifiable Credentials issued by government authorities. Verifiers can check credential status against this registry without contacting the original issuer.

Virtual Identifier (VID) Support: Integration with the VID system enabling citizens to use privacy-preserving virtual identifiers for blockchain interactions. VID mapping to underlying NIDs shall be maintained off-chain with only pseudonymous references on-chain.

5.2.4 NSOC Integration

All NBI components designated as Critical Information Infrastructure shall establish real-time monitoring connections with the National Security Operations Center (NSOC):

Security telemetry from validator nodes, RPC gateways, and administrative systems shall be streamed to NSOC for analysis and correlation with broader threat intelligence.

Anomaly detection alerts from NBI monitoring systems shall be integrated with NSOC incident management workflows.

NSOC shall have read-only access to blockchain explorer interfaces and audit logs for security monitoring purposes.

5.3 Technical Standards

This section establishes the technical standards governing blockchain implementations under this Policy. Standards are organized by domain and shall be updated periodically by the NBTC to reflect technological evolution.

5.3.1 Identity Standards

Decentralized Identifiers: W3C Decentralized Identifiers (DID) v1.0 specification shall be adopted for blockchain-based identity. A Bangladesh-specific DID method (did:bd) shall be defined specifying how DIDs are created, resolved, updated, and deactivated on NBI.

Verifiable Credentials: W3C Verifiable Credentials Data Model v1.1 or later shall be adopted for credential issuance and verification. Credential schemas shall be registered in a national schema registry for interoperability.

Verifiable Presentations: W3C Verifiable Presentations specification shall be adopted for holder-generated credential presentations supporting selective disclosure.

Biometric Standards: ISO/IEC 19794 series for biometric data formats where biometric binding is required for high-assurance credentials.

5.3.2 Interoperability Standards

ISO/TC 307: Bangladesh shall adopt relevant ISO/TC 307 blockchain and distributed ledger technology standards as they are finalized, including vocabulary (ISO 22739), reference architecture, and security standards.

Inter-Blockchain Communication: For cross-chain interoperability requirements, Inter-Blockchain Communication (IBC) protocol or equivalent standards providing light client verification and authenticated message passing shall be adopted. For value transfer between distinct blockchain networks, Atomic Swap protocols utilizing Hash Time-Locked Contracts (HTLC) shall be implemented to enable secure asset exchange without reliance on trusted intermediaries.

Financial Messaging: ISO 20022 financial messaging standards shall be adopted for blockchain applications involving payment or settlement to ensure interoperability with existing financial infrastructure.

API Standards: OpenAPI 3.0 specifications for RESTful API definitions. JSON-RPC 2.0 for blockchain node interfaces. GraphQL may be supported for complex query requirements.

5.3.3 Cryptographic Standards

Hash Functions: SHA-256 and SHA-3 (Keccak-256) are approved hash functions for integrity verification and commitment schemes. MD5 and SHA-1 shall not be used for security-critical applications.

Digital Signatures: ECDSA with secp256k1 curve (Ethereum compatible) or Ed25519 (EdDSA) for digital signatures. RSA signatures with minimum 2048-bit keys may be used for legacy integration but are not preferred for new implementations.

Encryption: AES-256-GCM for symmetric encryption of off-chain data. ECIES or equivalent for asymmetric encryption where required.

Key Derivation: BIP-32/BIP-39 hierarchical deterministic key derivation for wallet implementations. HKDF for general key derivation requirements.

Zero-Knowledge Proofs: ZK-SNARKs and ZK-STARKs may be employed for privacy-preserving verification. Trusted setup ceremonies for ZK-SNARKs shall follow documented multi-party computation procedures with audit trails.

Post-Quantum Readiness: The NBTC shall monitor NIST post-quantum cryptography standardization and develop migration plans for quantum-resistant algorithms. Hybrid schemes combining classical and post-quantum algorithms may be piloted for high-assurance applications.

5.3.4 Smart Contract Standards

Development Standards: Smart contracts for government deployment shall follow established security patterns including checks-effects-interactions, reentrancy guards, and access control modifiers. Contracts shall be developed using current stable compiler versions with optimization settings documented.

Token Standards: ERC-20 for fungible tokens and ERC-721/ERC-1155 for non-fungible tokens where tokenization is required. Government-specific token standards may be defined for specialized requirements.

Upgradability: Smart contracts requiring upgradability shall implement transparent proxy patterns or UUPS (Universal Upgradeable Proxy Standard) patterns. Upgrade governance including timelock delays, multisig requirements, and public notification procedures shall be documented.

Source Verification: All smart contracts deployed on NBI shall have verified source code published, enabling independent security review. Source verification workflows shall confirm that deployed bytecode matches published source.

Security Audits: Smart contracts processing government data or high-value operations shall undergo independent security audits by NBTC-certified auditors before deployment. Audit reports shall be published and remediation of identified issues verified.

Formal Verification: Critical smart contracts including core registry contracts, treasury contracts, and contracts with irreversible effects shall undergo formal verification mathematically proving correctness properties.

5.4 Privacy-Preserving Architecture

This section details the technical architecture for ensuring PDPO compliance while leveraging blockchain capabilities.

5.4.1 Off-Chain Data Storage Pattern

The mandatory architectural pattern for personal data is off-chain storage with on-chain integrity anchoring:

Data Vaults: Personal data shall be stored in encrypted data vaults operated by authorized Data Fiduciaries. Data vaults shall implement access controls, encryption at rest using AES-256, and comprehensive audit logging. Vaults shall be integrated with NRDEX for governed data sharing.

Hash Pointers: Only cryptographic hashes of personal data shall be stored on-chain. The hash serves as an integrity anchor enabling verification that data has not been modified since the hash was recorded. Hash pointers shall use approved hash functions (SHA-256 or SHA-3).

Metadata Separation: On-chain records shall contain minimal metadata necessary for functionality. Metadata that could enable re-identification when combined with other sources shall be kept off-chain.

5.4.2 Crypto-Shredding Implementation

Crypto-shredding provides effective data erasure while maintaining blockchain integrity:

Encryption Architecture: Off-chain personal data shall be encrypted using unique per-record encryption keys. Key management systems shall maintain secure key storage with access controls limiting key retrieval to authorized processes.

Erasure Procedure: Upon receipt of a valid erasure request under PDPO Section 12, the Data Fiduciary shall: (1) Verify the identity and authority of the requestor; (2) Locate all copies of the relevant data including backups; (3) Securely delete the encryption key using cryptographic erasure procedures; (4) Delete the encrypted data from all storage locations; (5) Record the erasure event in audit logs; (6) Confirm erasure completion to the data subject.

Verification: Following crypto-shredding, the hash pointer remaining on-chain references data that is mathematically inaccessible. Verification procedures shall confirm that the encryption key has been irrecoverably destroyed and the data cannot be decrypted.

5.4.3 Pseudonymization Techniques

Rotating DIDs: Citizens interacting with blockchain systems shall use rotating Decentralized Identifiers, generating fresh DIDs for different transaction contexts. This prevents creation of comprehensive activity profiles tied to persistent identifiers.

Sectoral Identifiers (SID): Domain-specific pseudonymous identifiers shall be used for sector-specific interactions. A citizen's SID for health services shall be unlinkable to their SID for land services without access to the mapping maintained in secured systems.

Zero-Knowledge Verification: Zero-knowledge proofs shall be employed where possible to verify attributes (such as age over 18, residency in a district, or possession of a valid credential) without revealing underlying identity information.

5.5 Security Architecture

The security architecture for blockchain systems shall implement defense-in-depth principles with multiple layers of controls.

5.5.1 Key Management

Hardware Security Modules: Validator signing keys and other critical cryptographic keys shall be generated, stored, and used within Hardware Security Modules (HSMs) meeting FIPS 140-2 Level 3 or equivalent certification. HSMs provide tamper-resistant protection against key extraction.

Multi-Party Computation: For high-value operations including treasury management and critical governance actions, Multi-Party Computation (MPC) shall be employed. MPC distributes key material across multiple parties such that no single party possesses the complete key, eliminating single points of compromise.

Key Ceremonies: Generation of root keys and trust anchors shall follow documented key ceremony procedures with multi-party controls, witness participation, and comprehensive audit trails. Key ceremonies shall be conducted in physically secured environments.

Key Rotation: Cryptographic keys shall be rotated according to defined schedules. Validator keys shall be rotated annually at minimum. Compromised keys shall be immediately revoked and replaced following incident response procedures.

5.5.2 Node Security

Hardened Operating Systems: Blockchain nodes shall run on hardened operating systems with unnecessary services disabled, security patches applied promptly, and configuration baselines enforced.

Network Segmentation: Node infrastructure shall implement network micro-segmentation isolating validator nodes, RPC endpoints, key management systems, and administrative interfaces in separate network segments with controlled inter-segment communication.

Endpoint Protection: Endpoint Detection and Response (EDR) solutions shall be deployed on all node infrastructure and administrator workstations, providing continuous monitoring for suspicious activity and supporting incident investigation.

Access Controls: Administrative access to node infrastructure shall require multi-factor authentication, use privileged access management (PAM) systems, and be logged for audit purposes. Just-in-time access provisioning shall be implemented where feasible.

5.5.3 Smart Contract Security

Secure Development Lifecycle: Smart contract development shall follow secure software development lifecycle (SSDLC) practices including threat modeling, secure coding guidelines, code review, testing, and security assessment.

Testing Requirements: Smart contracts shall undergo comprehensive testing including unit tests achieving high code coverage, integration tests, and property-based fuzzing using tools such as Echidna to discover edge cases.

Static Analysis: Automated static analysis tools such as Slither and Mythril shall be employed to identify common vulnerability patterns including reentrancy, integer overflow, and access control issues.

Audit Requirements: Smart contracts processing government data or exceeding defined value thresholds shall undergo independent security audits by qualified auditors. The NBTC shall maintain a registry of certified smart contract auditors meeting defined competency criteria.

Bug Bounty Programs: Public-facing smart contracts shall be covered by bug bounty programs incentivizing responsible vulnerability disclosure. Bounty amounts shall be proportional to severity and potential impact.

5.5.4 Incident Response

Detection Capabilities: Security Information and Event Management (SIEM) systems shall aggregate logs from all blockchain infrastructure components, applying correlation rules and anomaly detection to identify potential security incidents.

Response Procedures: Documented incident response procedures shall define roles, escalation paths, and response actions for different incident categories. Procedures shall be coordinated with NCERT and NSOC frameworks.

Reporting Requirements: Security incidents affecting CII-designated blockchain systems shall be reported to NCERT within timeframes prescribed by NCSA regulations. Initial notification shall occur within 6 hours of incident detection, with detailed reports within 72 hours.

Recovery Procedures: Business continuity and disaster recovery procedures shall enable restoration of blockchain services within defined RTO/RPO parameters. Regular recovery testing shall validate procedure effectiveness.

5.5.5 Vulnerability Management

Vulnerability Assessment: Regular vulnerability assessments shall be conducted on all blockchain infrastructure including network penetration testing, application security testing, and configuration review.

Penetration Testing: Annual penetration testing by qualified third parties shall assess the security posture of NBI infrastructure. Testing scope shall include network, application, and social engineering vectors.

Patch Management: Security patches for blockchain client software, operating systems, and dependencies shall be evaluated and applied within defined timeframes based on severity. Critical vulnerabilities shall be addressed within 72 hours.

CHAPTER 6: PRIORITY APPLICATION DOMAINS

This chapter identifies and details the priority application domains for blockchain deployment in Bangladesh. These domains have been selected based on alignment with national development priorities, potential for transformative impact, technical feasibility, and readiness of stakeholder ecosystems. For each domain, this chapter specifies the use cases, technical requirements, stakeholder responsibilities, and expected outcomes.

6.1 Digital Identity and Credential Verification

Digital identity represents the foundational application domain for blockchain, enabling trusted credential issuance, verification, and citizen empowerment through Self-Sovereign Identity principles.

6.1.1 Rationale and Alignment

Bangladesh's digital identity ecosystem anchored in the National Identity (NID) system presents significant opportunities for blockchain enhancement. The NDGO establishes the Unified Identity Layer concept, and the PDPO grants citizens ownership of their personal data. Blockchain-based Verifiable Credentials enable citizens to hold and present credentials from government issuers without requiring real-time connectivity to issuer systems, supporting the data ownership principles of the PDPO.

6.1.2 Use Cases

National DID Registry: A national Decentralized Identifier registry on NBI enabling citizens to control cryptographic identifiers. Citizens can create DIDs, register public keys, and manage DID Documents specifying service endpoints. The registry supports the Issuer-Holder-Verifier model for credential interactions.

Government Credential Issuance: Government agencies issue Verifiable Credentials for various entitlements and attestations including birth certificates, educational degrees, professional licenses, tax compliance certificates, and social protection eligibility. Credentials are cryptographically signed by issuers and can be verified without contacting the issuer.

Credential Status Verification: An on-chain credential status registry enabling verifiers to check whether credentials remain valid, have been suspended, or have been revoked. Status checks occur in real-time without revealing credential contents or holder identity to the registry.

Electronic Know Your Customer (E-KYC): Blockchain-enabled E-KYC enabling citizens to share verified identity attributes with financial institutions and service providers. Once verified by one institution, KYC attestations can be reused across institutions with citizen consent, reducing duplication and friction.

Citizen Credential Wallet: Mobile credential wallets enabling citizens to store Verifiable Credentials and present them to verifiers. Wallets shall support selective disclosure, enabling citizens to prove specific attributes without revealing complete credential contents.

6.1.3 Technical Requirements

W3C DID Core specification compliance with Bangladesh-specific DID method (did:bd). W3C Verifiable Credentials Data Model v1.1 for credential format. BBS+ signatures or similar for selective disclosure support. Credential schema registry for interoperability. Revocation registry using privacy-preserving mechanisms. Integration with NID system through secure APIs. Mobile wallet SDKs for iOS and Android platforms.

6.1.4 Stakeholder Responsibilities

The Election Commission shall serve as the trust anchor for identity binding to NID. Line ministries shall serve as credential issuers within their respective domains. The NDGA shall operate the DID registry and credential status infrastructure. The NBTC shall define credential schemas and interoperability profiles. Private sector entities may serve as verifiers upon authorization.

6.2 Land Records and Property Registration

Land administration represents a high-impact domain where blockchain can address endemic challenges of record integrity, fraud, and dispute resolution.

6.2.1 Rationale and Alignment

Bangladesh faces significant challenges in land administration including record fragmentation, mutation delays, forged deeds, and extensive litigation. The Ministry of Land has undertaken digitization initiatives, but fundamental challenges of data integrity and trust persist. Blockchain provides an immutable audit trail for land transactions, preventing unauthorized modifications and creating transparent ownership histories.

6.2.2 Use Cases

Property Chain: A permissioned blockchain recording the complete chain of title for land parcels. Each mutation, transfer, inheritance, partition, or encumbrance is recorded on-chain, creating an immutable history that can be audited and verified. The on-chain record contains hashes and references while actual deed documents remain in ministry systems.

Mutation Recording: When AC Land offices record mutations, the transaction is hashed and anchored to the blockchain. This creates tamper-evident proof that the mutation occurred at a specific time with specific details, protecting against subsequent unauthorized alterations.

Title Verification: Banks, buyers, and other parties can verify current ownership and encumbrance status through blockchain queries. The verification confirms that records have not been tampered with since recording, providing assurance for transactions and lending.

Dispute Evidence: In land disputes, blockchain records provide timestamped, tamper-evident evidence of the transaction history. Courts can rely on blockchain records as authoritative evidence of what records existed at specific points in time.

Digital Land Certificates: Landowners receive Verifiable Credentials representing their ownership rights. These credentials can be verified by any party without accessing central ministry systems, supporting transactions even in connectivity-limited areas.

6.2.3 Technical Requirements

Integration with existing Land Record Management Information System (LRMIS). Smart contracts for mutation workflow with multi-party approvals. Hash anchoring for deed documents stored in ministry systems. Verifiable Credentials for ownership certificates. Query interfaces for title verification services. Archive nodes for complete historical access. Integration with Sub-Registrar offices for deed registration. Compliance with Registration Act, 1908 and Transfer of Property Act, 1882. Implementation of Atomic Settlement mechanisms to ensure Delivery versus Payment (DvP), guaranteeing that ownership transfer and financial settlement occur simultaneously to eliminate counterparty risk in property transactions.

6.2.4 Stakeholder Responsibilities

The Ministry of Land shall serve as the primary authority and node operator. AC Land offices shall record mutations through authorized interfaces. Sub-Registrar offices shall record deed registrations. The Directorate of Land Records and Surveys shall maintain integration with cadastral systems. Courts shall have access for dispute resolution. Banks shall access verification services for lending decisions.

6.3 Educational Credential Verification

Educational credential verification addresses the persistent challenge of certificate fraud while enabling portable, verifiable academic credentials for students and graduates.

6.3.1 Rationale and Alignment

Certificate fraud undermines trust in Bangladesh's education system and disadvantages legitimate graduates in employment markets domestically and internationally. A blockchain-based Academic Chain, similar to India's Certificate Chain which has verified over 340 million documents, can eliminate fake degrees and streamline verification for employers.

6.3.2 Use Cases

Academic Credential Issuance: Universities and educational institutions issue degrees, diplomas, transcripts, and certificates as Verifiable Credentials. The credential hash is recorded on-chain while the full credential is held by the student.

Instant Verification: Employers can instantly verify the authenticity of academic credentials by checking the on-chain hash and verifying the issuer's digital signature. Verification occurs in seconds without contacting the issuing institution.

International Recognition: Verifiable academic credentials support international recognition and portability. Bangladeshi workers seeking employment abroad can present credentials that foreign employers can verify independently.

Secondary and Higher Secondary Certificates: Board examination results and certificates from Secondary School Certificate (SSC) and Higher Secondary Certificate (HSC) examinations are issued as Verifiable Credentials, creating verified academic histories from an early stage.

Professional Certifications: Professional bodies issue blockchain-verified certifications for engineers, doctors, accountants, and other regulated professions, enabling verification of professional qualifications.

6.3.3 Technical Requirements

W3C Verifiable Credentials with defined education credential schemas. Integration with university management information systems. Credential wallet applications for students. Verification portal and API for employers. Support for selective disclosure enabling verification of degree without revealing full transcript. Revocation capability for withdrawn degrees. Integration with international credential verification networks.

6.3.4 Stakeholder Responsibilities

The Ministry of Education shall provide policy oversight. The University Grants Commission shall coordinate university adoption. Education boards shall issue SSC/HSC credentials. Individual universities shall serve as credential issuers. The NBTC shall define credential schemas. Professional bodies shall issue professional certifications.

6.4 Public Finance and Procurement

Blockchain applications in public finance enhance transparency, accountability, and efficiency in government financial operations.

6.4.1 Rationale and Alignment

Public procurement and financial management require high levels of transparency and accountability. Blockchain provides immutable audit trails for financial transactions and procurement processes, supporting anti-corruption objectives and enabling real-time tracking of public expenditure.

6.4.2 Use Cases

Procurement Transparency: Public procurement processes are recorded on blockchain including tender announcements, bid submissions (encrypted until opening), evaluation results, and contract awards. The complete procurement history is transparent and auditable.

Contract Execution Tracking: Milestone completions, payment releases, and contract modifications for public contracts are recorded on-chain, creating transparent records of contract execution.

Budget Execution Monitoring: Budget allocations and expenditure records are anchored to blockchain, enabling real-time tracking of public spending against appropriations.

Subsidy Distribution: Distribution of government subsidies to beneficiaries is recorded on-chain, integrating directly with Mobile Financial Services (MFS) providers to ensure transparent last-mile delivery to citizen wallets identified by their DIDs and creating auditable records preventing duplicate payments and ensuring intended beneficiaries receive support.

Revenue Collection: Tax and revenue collection records are anchored to blockchain, creating tamper-evident receipts and supporting reconciliation between collection points and treasury.

6.4.3 Technical Requirements

Integration with iBAS++ (Integrated Budget and Accounting System). Integration with e-GP (Electronic Government Procurement) system. Smart contracts for procurement workflow automation. Hash anchoring for financial documents. Query interfaces for oversight bodies including OCAG (Office of the Comptroller and Auditor General). Treasury system integration for payment tracking.

6.4.4 Stakeholder Responsibilities

The Finance Division shall provide policy direction. The Controller General of Accounts shall integrate with iBAS++. CPTU (Central Procurement Technical Unit) shall integrate with e-GP. The National Board of Revenue shall participate for revenue tracking. OCAG shall have audit access. Planning Commission shall access for development project monitoring.

6.5 Supply Chain Management

Blockchain-enabled supply chain traceability addresses challenges of product authenticity, safety, and provenance across critical sectors.

6.5.1 Rationale and Alignment

Supply chain integrity is critical for public health (pharmaceuticals, food safety) and economic competitiveness (export documentation). Blockchain enables end-to-end traceability creating verified provenance records that prevent counterfeiting and support quality assurance.

6.5.2 Use Cases

Pharmaceutical Traceability: A Lab-to-Patient traceability system tracking pharmaceuticals from manufacturer through distributors to pharmacies. Each batch receives a digital identifier with blockchain-recorded movements, enabling verification of drug authenticity and preventing counterfeit medicines from entering the supply chain.

Agricultural Provenance: Farm-to-Fork traceability for agricultural products, recording origin, handling, processing, and distribution. Consumers can verify product authenticity and sourcing. Export products carry verified provenance supporting market access and premium pricing.

Export Documentation: Trade documents including certificates of origin, phytosanitary certificates, and quality inspection reports are issued as Verifiable Credentials. International trading partners can verify document authenticity without bilateral verification arrangements.

RMG (Ready-Made Garment) Traceability: Supply chain transparency for the garment sector, tracking materials from source through manufacturing. Supports compliance verification for sustainability and labor standards required by international buyers.

6.5.3 Technical Requirements

Digital twin creation for tracked items. IoT integration for automated checkpoint recording. QR code and RFID scanning at supply chain nodes. Integration with customs systems (ASYCUDA World). Compliance with international trade documentation standards. TradeTrust compatibility for transferable document interoperability. Consumer verification interfaces including mobile apps.

6.5.4 Stakeholder Responsibilities

The Ministry of Commerce shall oversee trade documentation. The Directorate General of Drug Administration shall participate for pharmaceutical traceability. Bangladesh Standards and Testing Institution shall participate for quality certification. Export Promotion Bureau shall coordinate export documentation. Private sector manufacturers and logistics providers shall participate as supply chain nodes.

6.6 Healthcare Data Exchange

Blockchain supports secure, consent-based health data exchange while protecting sensitive personal health information.

6.6.1 Rationale and Alignment

Health data is classified as sensitive personal data under PDPO Section 6, requiring enhanced protection. Blockchain enables patient-controlled health data sharing where citizens authorize access to their health records while maintaining audit trails of all access events.

6.6.2 Use Cases

Health Credential Issuance: Health facilities issue Verifiable Credentials for vaccination records, medical fitness certificates, and health screening results. Patients hold credentials in health wallets and present them when needed.

Consent-Based Data Sharing: Patients grant consent for specific healthcare providers to access their records. Consent grants and revocations are recorded on-chain, creating auditable consent histories. Data access events are logged.

Prescription Tracking: Prescriptions for controlled substances are tracked on blockchain, preventing duplicate prescriptions and supporting drug utilization monitoring.

Insurance Claims: Health insurance claims are processed with blockchain verification of treatment records, reducing fraud and accelerating claim settlement.

6.6.3 Technical Requirements

Strict PDPO Section 6 compliance for sensitive personal data. Enhanced encryption and access controls. Granular consent management. Health information exchange (HIE) standards including HL7 FHIR. Integration with hospital information systems. Patient-controlled health wallet applications. Audit logging for all data access events.

6.6.4 Stakeholder Responsibilities

The Ministry of Health and Family Welfare shall provide policy oversight. The Directorate General of Health Services shall coordinate public health facilities. Private hospitals and clinics shall participate as data sources and credential issuers. Health insurance companies shall participate for claims processing. The Drug Administration shall participate for prescription tracking.

CHAPTER 7: LEGAL LANDSCAPE AND REGULATORY POSITION

This chapter addresses the legal implications of blockchain technology in Bangladesh, including the evidentiary status of blockchain records, legal recognition of smart contracts, regulatory treatment of digital assets outside ICTD jurisdiction, and the liability framework for blockchain participants.

7.1 Evidentiary Status of Blockchain Records

The evidentiary treatment of blockchain records in legal proceedings requires clarification to ensure that the integrity benefits of blockchain technology translate into legal reliability.

7.1.1 Legal Framework for Electronic Evidence

The Information and Communication Technology Act, 2006 and the Evidence Act, 1872 (as amended) provide the foundational framework for electronic evidence in Bangladesh. Section 73A of the Evidence Act recognizes electronic records as admissible evidence, while Section 84 addresses presumptions regarding electronic records produced by computers.

Blockchain records constitute electronic records under this framework. However, the distributed and immutable nature of blockchain creates unique evidentiary characteristics that warrant specific treatment.

7.1.2 Blockchain Records as Evidence

Blockchain records shall be admissible as evidence in legal proceedings subject to the following considerations:

Integrity Presumption: Records stored on a blockchain that implements cryptographic linking and distributed consensus may benefit from a presumption of integrity. The mathematical properties of cryptographic hashing make undetected tampering computationally infeasible. This presumption may be rebutted by evidence of network compromise or consensus failure.

Timestamp Evidence: Blockchain timestamps provide evidence that specific data existed at a particular point in time. The timestamp is established by block inclusion time and network consensus. This supports proof of existence, priority, and temporal sequencing claims.

Chain of Custody: Blockchain provides transparent chain of custody for recorded events. Each transaction shows the submitting address, timestamp, and content hash, supporting authentication and provenance claims.

Expert Testimony: Courts may require expert testimony to explain blockchain technology and interpret blockchain evidence. The NBTC shall maintain a registry of qualified blockchain experts available for court testimony.

7.1.3 Evidentiary Weight

The evidentiary weight of blockchain records shall depend on:

- The security and governance of the specific blockchain network (permissioned government networks may carry greater weight than public networks with unknown validators).
- The completeness and accuracy of information recorded (blockchain guarantees integrity of recorded data but not accuracy of source data; garbage-in-garbage-out limitations apply).
- The relationship between on-chain records and off-chain data (hash pointers prove existence and integrity of off-chain data but require the off-chain data itself for content).
- Corroborating evidence supporting the blockchain record.

7.2 Legal Recognition of Smart Contracts

Smart contracts present novel questions regarding contract formation, enforceability, and the relationship between code and legal intent.

7.2.1 Smart Contract Definition

For legal purposes, a smart contract is computer code deployed on a blockchain that executes automatically when predefined conditions are met. Smart contracts may implement some or all terms of a legal agreement, or may operate independently as automated processes.

Smart contracts are not inherently legal contracts. Whether a smart contract constitutes a legally binding agreement depends on whether the elements of contract formation (offer, acceptance, consideration, intention to create legal relations, certainty of terms) are satisfied.

7.2.2 Contract Formation

Smart contracts may evidence contract formation where:

- The parties have manifested intent to be bound by the smart contract execution (through explicit agreement, course of dealing, or circumstances indicating acceptance).
- The terms embodied in the smart contract code are sufficiently certain and complete.
- Consideration is provided (which may include digital assets transferred through the smart contract).
- The subject matter and purpose are lawful.

7.2.3 Code as Contract Terms

Where parties agree that smart contract code shall govern their relationship, the code becomes part of the contractual terms. However, this presents interpretive challenges:

Code-Text Discrepancy: Where smart contract code and natural language contract terms conflict, the natural language terms shall generally prevail unless parties have expressly agreed to code primacy. Parties deploying smart contracts are advised to ensure consistency between code and written terms.

Bug and Exploit: Unintended code behavior (bugs) or exploitation of vulnerabilities does not automatically constitute valid contract performance. Parties may seek remedies where code execution diverges from agreed intent due to defects.

Immutability Limitations: The immutable execution of smart contracts does not preclude legal remedies. Courts may order parties to take corrective actions, provide compensation, or reverse effects of smart contract execution where legal grounds exist.

7.2.4 Jurisdictional Considerations

Smart contracts deployed on the National Blockchain Infrastructure and involving parties within Bangladesh shall be subject to Bangladeshi law unless parties validly agree to alternative governing law. Smart contracts with international elements may raise choice of law questions to be resolved under applicable conflict of laws principles.

7.3 Digital Signatures and Authentication

Blockchain transactions are authenticated through digital signatures using public key cryptography. The legal status of these signatures is addressed by existing electronic signature frameworks.

7.3.1 Electronic Signature Recognition

The Information and Communication Technology Act, 2006 recognizes electronic signatures as legally valid. Blockchain digital signatures (such as ECDSA signatures) constitute electronic signatures under this framework when:

- The signature is uniquely linked to the signatory (through private key control).
- The signature is capable of identifying the signatory (through public key verification).
- The signature is created using means under the signatory's sole control.
- The signature is linked to data in such manner that any subsequent change is detectable (inherent in blockchain transaction structure).

7.3.2 Attribution and Non-Repudiation

Blockchain signatures provide strong technical non-repudiation: a valid signature can only be produced by someone possessing the private key. However, legal attribution requires establishing that the purported signatory controlled the private key at the relevant time. Key management practices, custody arrangements, and evidence of key compromise affect attribution analysis.

7.4 Regulatory Position on Crypto Assets and Virtual Currencies

This section clarifies the regulatory treatment of crypto assets, virtual currencies, and related activities, which fall outside the scope of this Policy and remain under the jurisdiction of their respective regulatory authorities.

7.4.1 Bangladesh Bank Authority

Bangladesh Bank retains exclusive authority over monetary and financial regulatory matters. The following activities require Bangladesh Bank authorization and are subject to Bangladesh Bank regulations:

Cryptocurrency Trading and Exchange: The operation of cryptocurrency exchanges, trading platforms, and over-the-counter trading desks for buying, selling, or exchanging cryptocurrencies is regulated by Bangladesh Bank. Entities conducting such activities must comply with licensing requirements, capital adequacy standards, and operational requirements as may be prescribed by Bangladesh Bank.

Virtual Asset Service Providers (VASPs): Entities conducting exchange between virtual assets and fiat currencies, exchange between forms of virtual assets, transfer of virtual assets, safekeeping or administration of virtual assets, and related financial services are classified as VASPs and subject to Bangladesh Bank's AML/CFT regulations pursuant to the Anti-Money Laundering Act, 2012 and Financial Action Task Force (FATF) recommendations.

Payment Services: Blockchain-based payment services, stored value facilities, and money transmission services require authorization under Bangladesh Bank's payment system regulations. Stablecoins used for payment purposes are subject to payment service regulations.

Central Bank Digital Currency (CBDC): Any digital currency issued by Bangladesh Bank representing sovereign currency remains exclusively within Bangladesh Bank's monetary policy authority. This Policy does not govern or affect Bangladesh Bank's prerogatives regarding CBDC development or issuance.

Foreign Exchange: Cross-border virtual asset transfers and cryptocurrency transactions involving foreign exchange are subject to the Foreign Exchange Regulation Act, 1947. Blockchain applications facilitating cross-border value transfer must comply with foreign exchange regulations.

7.4.2 Bangladesh Securities and Exchange Commission Authority

The Bangladesh Securities and Exchange Commission (BSEC) exercises jurisdiction over securities markets. The following blockchain-related activities fall under BSEC regulatory authority:

Security Tokens: Tokens representing equity, debt, revenue shares, or other investment interests constitute securities and are subject to securities regulations including registration, disclosure, and trading requirements under the Securities and Exchange Ordinance, 1969.

Security Token Offerings: Public offerings of security tokens must comply with prospectus requirements, investor protection rules, and other applicable securities regulations. Exemptions available for traditional securities offerings apply to security token offerings.

Investment Schemes: Collective investment schemes using blockchain technology, including decentralized autonomous organizations (DAOs) pooling investor funds, may constitute collective investment schemes subject to BSEC regulation.

Market Infrastructure: Blockchain-based trading systems, clearing and settlement infrastructure, and securities depositories require BSEC authorization and must comply with market infrastructure regulations.

7.4.3 Ministry of Commerce Authority

The Ministry of Commerce retains authority over trade and commerce matters affecting blockchain applications:

Consumer Protection: Consumer protection requirements apply to blockchain-based commerce including disclosure obligations, product safety requirements, and remedies for defective goods or services sold using blockchain verification.

Trade Documentation: Blockchain-based trade documents including bills of lading, certificates of origin, and letters of credit are subject to applicable trade documentation requirements and international trade law.

E-Commerce Regulations: E-commerce transactions using blockchain technology are subject to applicable e-commerce regulations including those governing electronic contracts, consumer rights, and dispute resolution.

7.5 Liability Framework

This section establishes the liability framework for participants in blockchain ecosystems operating under this Policy.

7.5.1 Validator Node Operator Liability

Entities operating validator nodes on the National Blockchain Infrastructure assume responsibilities and potential liabilities:

Operational Obligations: Validators must maintain node availability, apply security updates, participate in consensus honestly, and comply with governance requirements. Failure to meet operational obligations may result in removal from the validator set and potential liability for resulting damages.

Security Liability: Validators are responsible for securing their node infrastructure and key material. Negligent security practices leading to key compromise or node exploitation may result in liability for resulting losses.

Consensus Participation: Validators participating in consensus must do so honestly. Malicious behavior including double-signing, censorship, or collusion to manipulate consensus may result in penalties and liability.

Fair Ordering: Validators are strictly prohibited from engaging in Maximal Extractable Value (MEV) extraction techniques, such as front-running, sandwich attacks, or arbitrary transaction reordering for profit. Detected MEV activity shall constitute grounds for immediate revocation of validator status.

7.5.2 Smart Contract Deployer Liability

Entities deploying smart contracts on NBI bear responsibility for contract correctness and security:

Code Quality: Deployers are responsible for ensuring smart contracts function as intended and do not contain exploitable vulnerabilities. Deployers must conduct appropriate testing and obtain required security audits before deployment.

Upgrade Governance: Deployers of upgradeable contracts bear ongoing responsibility for proper upgrade governance including security review of upgrades and appropriate notice to users.

Data Protection: Smart contracts processing personal data must comply with PDPO requirements. Deployers bear Data Fiduciary responsibilities for personal data processed through their contracts.

7.5.3 Data Fiduciary Obligations

Entities processing personal data through blockchain systems are Data Fiduciaries under the PDPO and bear corresponding obligations:

- Obtaining and maintaining valid consent for data processing.
- Implementing privacy-preserving architectures including off-chain storage and crypto-shredding.

- Responding to data subject requests for access, correction, and erasure.
- Reporting data breaches to affected data subjects and the NDGA within prescribed timeframes.
- Conducting Data Protection Impact Assessments for high-risk processing activities.

7.5.4 Limitation of Liability

Blockchain technology introduces novel liability considerations. The following principles guide liability allocation:

Protocol Layer: The NBI protocol layer operated by the NDGA provides infrastructure services. The NDGA shall not be liable for applications built on NBI or for losses resulting from user error, application bugs, or third-party attacks not caused by protocol defects or NDGA negligence.

Application Layer: Application developers and deployers bear primary liability for their applications. Users interacting with applications assume risks inherent in the specific application, subject to consumer protection requirements.

Force Majeure: Blockchain participants shall not be liable for failures caused by force majeure events including natural disasters, war, government action, or circumstances beyond reasonable control, provided reasonable mitigation efforts were undertaken.

7.6 Dispute Resolution

Disputes arising from blockchain transactions may be resolved through:

On-Chain Mechanisms: Some smart contracts implement on-chain dispute resolution through arbitration protocols or governance voting. Where parties have agreed to such mechanisms, they may be binding subject to legal validity.

Alternative Dispute Resolution: Mediation and arbitration remain available for blockchain disputes. Specialized arbitrators with blockchain expertise may be designated for technology-related disputes.

Court Jurisdiction: Courts retain jurisdiction over blockchain disputes. Parties cannot exclude court jurisdiction through smart contract terms. Courts may issue orders requiring parties to take on-chain actions, reverse transactions, or provide compensation.

Grievance Redress: Government blockchain services shall maintain grievance redress mechanisms enabling citizens to raise complaints about service delivery, data handling, or technical issues. Grievances shall be addressed within prescribed timelines.

CHAPTER 8: IMPLEMENTATION FRAMEWORK

8.1 Implementation Principles

The implementation of this Policy shall be guided by the following principles:

Phased Approach: Implementation shall proceed through defined phases, with each phase building upon the foundations established by preceding phases. This approach enables learning from early deployments, allows course corrections, and ensures that complex initiatives are not undertaken before prerequisite capabilities are in place.

Pilot-First Methodology: New blockchain applications shall be piloted in controlled environments before scaling to production deployments. Pilots enable validation of technical approaches, identification of integration challenges, and refinement of operational procedures.

Interoperability by Design: All implementations shall be designed for interoperability from the outset, adhering to the technical standards established in Chapter 5 and ensuring integration with the Bangladesh National Digital Infrastructure Architecture (BNDIA).

Stakeholder Engagement: Implementation shall involve continuous engagement with stakeholders including government agencies, private sector entities, civil society, and citizens. Feedback mechanisms shall inform iterative improvements.

Sustainability Focus: Implementations shall be designed for long-term sustainability, including operational cost management, skills development for ongoing maintenance, and governance structures that endure beyond initial project phases.

8.2 Phased Implementation Roadmap

The implementation roadmap spans five years (2026-2030), organized into three primary phases aligned with the National Digital Transformation Strategy phases.

8.2.1 Phase 1: Foundation (2026-2027)

Phase 1 establishes the institutional, technical, and regulatory foundations for blockchain deployment in Bangladesh.

Institutional Setup (Q1-Q2 2026): Establish the National Blockchain Technical Committee (NBTC) under NDGA. Appoint NBTC members from ICT Division, Bangladesh Computer Council, line ministries, academia, and industry. Define NBTC operating procedures and meeting schedules. Establish the Blockchain Division within NDGA's Technical Standards and Interoperability Division.

Regulatory Framework (Q2-Q3 2026): Issue implementing rules and regulations for this Policy. Publish technical guidelines for blockchain platform evaluation and approval. Establish node operator eligibility criteria and application procedures. Define smart contract audit requirements and auditor certification criteria.

National Blockchain Infrastructure Setup (Q3-Q4 2026): Deploy initial NBI validator nodes at National Data Center and BDCCL facilities. Establish network configuration and consensus parameters. Deploy core smart contracts including DID registry and credential status registry. Establish RPC gateway infrastructure with authentication and monitoring.

Pilot Applications (Q4 2026 - Q2 2027): Launch digital identity pilot with DID issuance and Verifiable Credential demonstration. Initiate educational credential verification pilot with selected universities. Begin land records pilot in selected upazilas with Ministry of Land. Evaluate pilot outcomes and document lessons learned.

Capacity Building Initiation (Throughout Phase 1): Conduct blockchain fundamentals training for NDGA and line ministry staff. Train initial cohort of smart contract developers. Establish relationships with academic institutions for curriculum development. Begin public awareness campaigns on blockchain benefits and citizen services.

8.2.2 Phase 2: Scale and Optimization (2027-2028)

Phase 2 focuses on scaling successful pilots, expanding the NBI network, and deploying production applications across priority domains.

NBI Expansion (Q1-Q4 2027): Expand validator network to include nodes operated by major line ministries (Land, Education, Health, Finance). Integrate NBI with NRDEX through oracle infrastructure. Deploy archive nodes for regulatory and audit purposes. Establish disaster recovery capabilities with synchronized replica at DR site.

Production Deployments (Q2 2027 - Q4 2028): Launch national DID registry for government credential issuance. Deploy Academic Chain for educational credential verification nationally. Expand land records blockchain to additional districts based on pilot learnings. Launch public finance transparency applications for procurement and budget tracking. Initiate supply chain pilots for pharmaceuticals and agricultural products.

Ecosystem Development (Throughout Phase 2): Establish Blockchain Regulatory Sandbox for private sector innovation. Certify initial cohort of smart contract auditors. Launch blockchain developer certification program. Engage private sector for application development partnerships. Establish Bangladesh Blockchain Centre of Excellence for research and development.

Integration and Interoperability (Q3 2027 - Q4 2028): Complete SITA Gateway integration enabling blockchain verification services. Integrate with Unified Identity Layer for NID-DID binding. Establish cross-border credential verification pilots with regional partners. Adopt TradeTrust compatibility for trade documentation.

8.2.3 Phase 3: Consolidation and Advanced Applications (2029-2030)

Phase 3 consolidates achievements, deploys advanced applications, and positions Bangladesh as a regional leader in government blockchain adoption.

Advanced Infrastructure (2029): Deploy Layer 2 scaling solutions if transaction volume requires. Implement advanced privacy features including zero-knowledge proof applications. Establish cross-chain interoperability with approved external networks. Achieve full NSOC integration for all CII-designated blockchain components.

Comprehensive Application Coverage (2029-2030): National coverage for land records blockchain across all districts. Full integration of educational credentials from SSC through higher education. Healthcare data exchange pilot expanding to production. Comprehensive supply chain coverage for priority export sectors. Public finance transparency across all major procurement categories.

Regional Leadership (2030): Establish bilateral credential recognition agreements with regional partners. Participate in international blockchain governance forums. Share implementation experience through South-South cooperation. Position Bangladesh as reference implementation for government blockchain in developing countries.

Sustainability Achievement (2030): Achieve operational sustainability with defined funding mechanisms. Complete knowledge transfer ensuring government self-sufficiency. Establish mature governance processes with documented procedures. Transition from project-based to operational mode.

8.3 Institutional Arrangements

Effective implementation requires clear institutional arrangements with defined roles and coordination mechanisms.

8.3.1 Governance Structure

National Data Governance Policy Board: Chaired by the Chief Adviser, the Policy Board provides highest-level oversight for blockchain initiatives as part of broader data governance. The Board receives quarterly progress reports and provides strategic direction on major policy matters.

National Data Governance Authority (NDGA): NDGA serves as the primary implementing authority with responsibility for NBI operation, node operator authorization, compliance monitoring, and technical guideline development. The NDGA Blockchain Division manages day-to-day operations.

National Blockchain Technical Committee (NBTC): NBTC provides technical expertise and recommendations on platform evaluation, standards development, and technology evolution. NBTC meets monthly and maintains working groups for specific technical domains.

Implementation Steering Committee: A Blockchain Implementation Steering Committee chaired by the Secretary, ICT Division, with representation from implementing ministries, coordinates cross-agency implementation efforts. The Committee meets quarterly to review progress, resolve issues, and approve workplans.

Sectoral Implementation Units: Each implementing ministry shall establish a Blockchain Implementation Unit led by a designated focal point. Units are responsible for ministry-specific implementation activities, user training, and change management.

8.3.2 Coordination Mechanisms

Inter-Agency Working Groups: Technical working groups bringing together implementers across ministries address specific challenges including identity integration, data standards harmonization, and security coordination.

Private Sector Engagement: Regular consultations with private sector stakeholders including technology providers, industry associations (BASIS, BACCO), and potential application users inform implementation and identify collaboration opportunities.

Academic Partnership: Formal partnerships with universities support research, curriculum development, and talent pipeline creation.

8.4 Risk Management

Implementation involves technical, organizational, and external risks requiring proactive management.

8.4.1 Technical Risks

Risk	Impact	Probability	Mitigation Strategy
Technology Obsolescence	High	Medium	Technology-neutral standards; modular architecture; regular technology review by NBTC
Security Breaches	Critical	Medium	Defense-in-depth security; HSM key protection; continuous monitoring; incident response plans
Performance/Scalability Issues	High	Medium	Performance testing before deployment; capacity planning; Layer 2 scaling readiness
Integration Failures	High	Medium	Standardized APIs; comprehensive testing; phased integration approach
Smart Contract Vulnerabilities	High	Medium	Mandatory audits; formal verification for critical contracts; bug bounty programs

8.4.2 Organizational Risks

Risk	Impact	Probability	Mitigation Strategy
Institutional Resistance	High	High	Change management programs; leadership engagement; demonstration of benefits
Skills Gap	High	High	Comprehensive capacity building; competitive compensation; knowledge transfer requirements
Coordination Failures	Medium	Medium	Clear governance structures; regular coordination meetings; escalation procedures
Funding Constraints	High	Medium	Diversified funding sources; phased investments; efficiency optimization
Political Discontinuity	Medium	Low	Institutional embedding; cross-party awareness; demonstrated public value

8.4.3 External Risks

Risk	Impact	Probability	Mitigation Strategy
Regulatory Changes	Medium	Medium	Flexible architecture; engagement with other regulators; proactive compliance
Global Technology Shifts	Medium	Medium	Technology monitoring; participation in standards bodies; architecture flexibility
Vendor Dependencies	High	Medium	Open standards mandate; multi-vendor strategy; open-source preference
Cybersecurity Threats	Critical	High	Continuous threat monitoring; incident response capabilities; international cooperation

8.5 Blockchain Regulatory Sandbox

A Blockchain Regulatory Sandbox shall be established to enable controlled experimentation with blockchain applications while managing risks.

8.5.1 Sandbox Objectives

Enable private sector innovation by providing a controlled environment for testing blockchain applications before full regulatory compliance is required. Allow regulators to understand emerging business models and develop appropriate regulatory responses. Identify promising applications for potential government adoption or partnership. Build ecosystem capabilities and attract blockchain investment to Bangladesh.

8.5.2 Sandbox Governance

The NDGA shall administer the sandbox with support from the NBTC. Sectoral regulators (Bangladesh Bank, BSEC, etc.) shall participate in evaluating sandbox applications within their regulatory domains. The sandbox shall operate through defined cohorts, with applications accepted during defined application windows and evaluated against published criteria.

8.5.3 Sandbox Parameters

Eligibility: Private companies, startups, academic institutions, and government agencies may apply for sandbox participation. Applications must demonstrate genuine innovation, clear testing objectives, consumer protection measures, and an exit strategy.

Duration: Sandbox participation shall be limited to 12 months with possibility of extension for up to 6 additional months based on demonstrated progress.

Restrictions: Sandbox applications involving financial services, payment systems, or activities regulated by Bangladesh Bank or BSEC shall require concurrent approval from those regulators. Consumer protection requirements remain applicable within the sandbox.

Reporting: Sandbox participants shall provide monthly progress reports and final evaluation reports documenting outcomes, lessons learned, and regulatory recommendations.

CHAPTER 9: CAPACITY BUILDING AND ECOSYSTEM DEVELOPMENT

This chapter establishes the comprehensive capacity building framework to develop the human capital, institutional capabilities, and ecosystem infrastructure necessary for successful blockchain adoption in Bangladesh. The framework addresses multiple stakeholder groups and builds upon existing digital skills development initiatives.

9.1 Capacity Building Objectives

The capacity building framework aims to achieve the following objectives by 2030:

- Develop a pool of blockchain developers with competencies ranging from smart contract development to protocol engineering, capable of building and maintaining government blockchain applications.
- Train government officials across line ministries and agencies on blockchain concepts, applications, and operational procedures relevant to their functional domains.
- Certify smart contract auditors meeting NBTC competency standards, providing adequate audit capacity for government and private sector applications.
- Establish blockchain curricula in universities and technical institutions, creating sustainable talent pipelines aligned with industry needs.
- Build citizen awareness enabling effective utilization of blockchain-enabled government services, particularly credential wallets and verification services.

9.2 Target Groups and Training Tracks

9.2.1 Track 1: Government Officials

Government officials require blockchain literacy appropriate to their roles, ranging from general awareness to technical proficiency.

Executive Awareness (Senior Officials): Half-day executive briefings for Secretaries, Additional Secretaries, and Joint Secretaries covering blockchain fundamentals, strategic implications, and policy considerations. Target: All senior officials in implementing ministries.

Functional Training (Mid-Level Officials): Two-day workshops for Deputy Secretaries, Directors, and equivalent officers covering blockchain applications in their functional domains, data governance integration, and change management.

Operational Training (Field Officers): Three-day hands-on training for field-level officers who will operate blockchain-enabled services, including AC Land officers, education board officials, and healthcare administrators. Training covers operational procedures, troubleshooting, and citizen support.

Technical Training (ICT Staff): Intensive technical training for ministry ICT staff covering NBI integration, API development, security practices, and system administration.

9.2.2 Track 2: Blockchain Developers

Developer training creates the technical workforce for blockchain application development and maintenance.

Foundation Program: Eight-week intensive program covering blockchain fundamentals, cryptography, distributed systems, and smart contract basics. Prerequisites: Programming experience. Delivery: Bangladesh Computer Council training centers and partner institutions.

Advanced Development Program: Twelve-week specialized program covering advanced Solidity development, security patterns, formal verification, testing frameworks, and deployment practices. Prerequisites: Foundation program completion.

Specialized Tracks: Four-week specialized modules in areas including DID/VC implementation, ZK proof development, Layer 2 solutions, and cross-chain interoperability.

Certification: Graduates completing programs and passing assessments receive NBTC-recognized blockchain developer certification, recognized for government project participation.

9.2.3 Track 3: Smart Contract Auditors

Smart contract auditors require specialized skills combining software security, blockchain domain knowledge, and formal methods expertise.

Auditor Certification Program: Sixteen-week intensive program covering smart contract vulnerability classes, static and dynamic analysis tools, manual review techniques, formal verification basics, and audit methodology. Prerequisites: Advanced development program or equivalent experience.

Practical Experience: Candidates must complete supervised audits of real-world contracts before full certification. Partnership with established audit firms provides mentorship and quality assurance.

Continuing Education: Certified auditors must complete annual continuing education covering emerging vulnerability patterns and new analysis techniques to maintain certification.

Registry: The NBTC shall maintain a public registry of certified auditors and audit firms eligible for government smart contract audits.

9.2.4 Track 4: Academic Integration

Sustainable blockchain skills development requires integration into formal academic programs.

Curriculum Development: Collaborate with University Grants Commission and leading universities to develop standardized blockchain curricula for computer science and related programs. Modules range from introductory blockchain concepts to advanced distributed systems courses.

Faculty Development: Train university faculty through dedicated faculty development programs enabling them to deliver blockchain courses.

Research Programs: Establish blockchain research programs at leading universities addressing challenges relevant to Bangladesh's deployment context. Government-funded research grants support relevant applied research.

Industry Partnerships: Facilitate industry-academia partnerships including internship programs, industry advisory boards for curriculum review, and collaborative research projects.

9.2.5 Track 5: Citizen Awareness

Citizens must understand blockchain-enabled services to effectively utilize them.

Public Awareness Campaigns: Mass media campaigns explaining blockchain benefits, credential wallet usage, and verification processes. Content delivered through television, radio, social media, and Union Digital Centers.

Service-Specific Education: When launching blockchain-enabled services, provide targeted education to service users. Example: When launching academic credential verification, educate students and employers on credential wallet usage.

Digital Literacy Integration: Integrate blockchain awareness into broader digital literacy programs delivered through Union Digital Centers and community information centers.

9.3 Institutional Framework for Capacity Building

9.3.1 Lead Institutions

Bangladesh Computer Council (BCC): BCC shall serve as the primary delivery institution for developer training programs, leveraging existing training infrastructure and expanding to include blockchain tracks. BCC regional offices shall deliver programs nationwide.

NDGA Training Wing: The NDGA shall establish a training wing responsible for government official training, developing training content, and maintaining training standards. Coordination with Bangladesh Public Administration Training Centre (BPATC) for senior official programs.

Partner Universities: Selected universities including BUET, DU, KUET, RUET, and SUST shall serve as academic partners for curriculum development, faculty training, and research programs.

9.3.2 International Partnerships

International partnerships shall supplement domestic capacity building:

- Bilateral programs with countries having advanced blockchain implementations (Singapore, South Korea, Estonia) for knowledge exchange and study visits.
- Engagement with international organizations (ITU, World Bank, ADB) supporting digital transformation for technical assistance and training resources.
- Partnerships with international blockchain foundations and consortia for access to training materials, certification programs, and community engagement.
- Participation in international blockchain governance forums building Bangladesh's expertise and influence in global standards development.

9.4 Ecosystem Development

Beyond individual skills, successful blockchain adoption requires a thriving ecosystem of service providers, innovators, and supporting infrastructure.

9.4.1 Private Sector Development

Blockchain Service Providers: Encourage development of local blockchain consulting firms, development shops, and managed service providers. Government procurement preferences for local firms meeting quality standards build domestic industry capabilities.

Startup Ecosystem: The Blockchain Regulatory Sandbox provides a pathway for blockchain startups to develop and test innovative applications. Incubation programs and venture funding support promising blockchain ventures.

Industry Associations: Support formation of blockchain-focused industry associations or working groups within existing associations (BASIS, BACCO) to coordinate industry development, represent industry perspectives, and promote standards adoption.

9.4.2 Innovation Infrastructure

Innovation Hubs: Blockchain-focused innovation hubs within Hi-Tech Parks provide co-working space, mentorship, and resources for blockchain entrepreneurs and researchers.

Hackathons and Challenges: Annual blockchain hackathons challenge developers to build solutions for government and social challenges. Winning solutions may be piloted through the regulatory sandbox.

Open Source Contributions: Encourage and recognize contributions to open source blockchain projects. Government-funded development shall prioritize open source releases benefiting the broader ecosystem.

CHAPTER 10: MONITORING, EVALUATION, AND REVIEW

This chapter establishes the framework for monitoring implementation progress, evaluating outcomes, and conducting periodic policy reviews. The framework ensures accountability, enables evidence-based decision making, and supports continuous improvement of blockchain initiatives.

10.1 Monitoring Framework

10.1.1 Monitoring Objectives

The monitoring framework aims to track implementation progress against planned milestones, identify deviations early enabling timely corrective action, provide data for resource allocation and prioritization decisions, ensure accountability of implementing agencies, and support transparency through public reporting.

10.1.2 Data Collection and Reporting

Automated Data Collection: Infrastructure and transaction metrics shall be collected automatically through blockchain analytics tools, monitoring systems, and administrative interfaces. Automated collection ensures accuracy and timeliness.

Implementing Agency Reports: Implementing ministries and agencies shall submit quarterly progress reports to the NDGA covering implementation activities, challenges encountered, and support requirements.

Blockchain Dashboard: A National Blockchain Dashboard shall provide real-time visualization of key metrics. The dashboard shall be accessible to policymakers and stakeholders, with selected metrics published for public transparency.

Reporting Cadence: Monthly operational reports for NDGA internal management. Quarterly progress reports for the Implementation Steering Committee. Semi-annual reports for the National Data Governance Policy Board. Annual public reports for transparency and accountability.

10.2 Evaluation Framework

10.2.1 Evaluation Objectives

Evaluation assesses whether blockchain initiatives achieve their intended outcomes and deliver value for citizens and government. Evaluation goes beyond activity tracking to examine effectiveness, efficiency, and impact.

10.2.2 Evaluation Methods

Quantitative Analysis: Statistical analysis of KPI data, transaction volumes, and outcome metrics provides quantitative evidence of performance and trends.

User Surveys: Periodic surveys of service users (citizens, businesses, government officials) assess satisfaction, usability, and perceived benefits.

Case Studies: In-depth case studies of specific implementations provide rich qualitative insights into implementation experiences, challenges, and success factors.

Independent Assessments: External evaluators from academic institutions, civil society, or international organizations provide independent perspectives on implementation progress and outcomes.

Benchmarking: Comparison with international implementations and best practices identifies improvement opportunities and validates approaches.

10.2.3 Evaluation Schedule

Evaluation Type	Frequency	Scope	Conducted By
Operational Review	Quarterly	Process efficiency, system performance	NDGA Internal
User Satisfaction Survey	Annual	Citizen and official satisfaction	Third-party research firm
Application Impact Evaluation	Biennial	Outcome achievement per application	Academic institution
Comprehensive Policy Evaluation	Every 3 years	Overall policy effectiveness	Independent evaluator
International Benchmarking	Every 2 years	Comparison with peer countries	International organization

10.3 Review Mechanisms

10.3.1 Policy Review

This Policy shall be subject to comprehensive review every three years to assess continued relevance, update provisions based on implementation experience, and incorporate technological and regulatory developments.

Scheduled Reviews: Comprehensive policy reviews scheduled for 2029 and 2032 shall examine all policy provisions, assess achievement of objectives, and propose amendments as needed.

Interim Updates: Technical guidelines, standards, and operational procedures may be updated between comprehensive reviews through NBTC recommendations approved by NDGA. Such updates shall not alter core policy provisions.

Review Process: Policy reviews shall involve stakeholder consultations, independent assessment of implementation, analysis of international developments, and public comment periods before finalization.

10.3.2 Technical Standards Review

Technical standards require more frequent review given rapid technology evolution:

Annual Standards Review: The NBTC shall conduct annual reviews of technical standards, assessing continued appropriateness and identifying update needs. Reviews shall consider international standards developments, security research, and implementation experience.

Emerging Technology Assessment: The NBTC shall continuously monitor emerging technologies (e.g., post-quantum cryptography, new consensus mechanisms, privacy-enhancing technologies) and recommend adoption timelines.

Security Updates: Security-related standards updates may be issued on an emergency basis in response to discovered vulnerabilities or threats, with expedited NBTC approval process.

10.3.3 Regulatory Sandbox Review

Sandbox operations shall be reviewed annually to assess effectiveness in promoting innovation while managing risks, identify regulatory gaps or needed clarifications, evaluate sandbox application outcomes, and recommend sandbox parameter adjustments.

10.4 Accountability Mechanisms

10.4.1 Implementing Agency Accountability

Implementing ministries and agencies shall be accountable for their blockchain implementation responsibilities through:

Performance Agreements: Annual performance agreements between NDGA and implementing agencies defining deliverables, milestones, and accountability measures.

Progress Reviews: Quarterly progress reviews with the Implementation Steering Committee providing opportunity to address challenges and ensure continued progress.

Escalation Procedures: Defined procedures for escalating persistent implementation challenges to higher authorities for resolution.

10.4.2 Public Accountability

Transparency Reports: Annual public reports on blockchain implementation progress, outcomes, and expenditure shall be published and disseminated.

Grievance Redress: Grievance redress mechanisms shall enable citizens to raise concerns about blockchain-enabled service delivery. Grievances shall be tracked, addressed within defined timelines, and analyzed for systemic improvement opportunities.

Civil Society Engagement: Regular engagement with civil society organizations provides independent perspectives on implementation and identifies citizen concerns.

10.4.3 Audit and Oversight

Internal Audit: NDGA internal audit functions shall include blockchain operations within their scope, assessing operational compliance, security practices, and resource utilization.

External Audit: The Office of the Comptroller and Auditor General (OCAG) shall have access to blockchain systems and records for external audit purposes. Smart contract expenditure, operational costs, and asset management shall be auditable.

Parliamentary Oversight: Parliamentary committees with jurisdiction over ICT and digital governance shall receive briefings on blockchain implementation and may request information or hearings as needed.

CHAPTER 11: CONCLUSION

The National Blockchain Policy of Bangladesh 2026 establishes a comprehensive framework for the responsible deployment of blockchain technology in support of national digital transformation objectives. This Policy positions Bangladesh to leverage blockchain's unique capabilities for enhancing trust, transparency, and efficiency in government services while maintaining strict compliance with data protection, privacy, and cybersecurity requirements.

11.1 Summary of Key Provisions

This Policy establishes a clear regulatory framework built upon the governance triad of the National Data Governance Ordinance, 2025, the Personal Data Protection Ordinance, 2025, and the Cyber Safety Ordinance, 2025. The National Data Governance Authority serves as the primary regulator for government blockchain deployments, with the National Blockchain Technical Committee providing specialized technical expertise and sectoral regulators retaining jurisdiction over domain-specific matters.

The technical architecture centers on the National Blockchain Infrastructure, a sovereign permissioned network operated by designated government entities under NDGA oversight. The architecture prioritizes privacy-preserving approaches with mandatory off-chain storage of personal data, crypto-shredding mechanisms for PDPO compliance, and zero-trust security principles aligned with CSO requirements.

Six priority application domains have been identified for blockchain deployment: digital identity and credential verification, land records and property registration, educational credential verification, public finance and procurement transparency, supply chain management, and healthcare data exchange. Each domain offers significant potential for improving citizen services while demonstrating blockchain value.

The legal framework addresses the evidentiary status of blockchain records, legal recognition of smart contracts, and regulatory treatment of crypto assets and virtual currencies. Matters falling under Bangladesh Bank, BSEC, or Ministry of Commerce jurisdiction remain subject to their respective regulatory frameworks.

Implementation follows a phased approach spanning 2026-2030, with comprehensive capacity building programs targeting 1,000 blockchain developers, 5,000 trained government officials, and 100 certified smart contract auditors. The Blockchain Regulatory Sandbox enables controlled innovation while managing risks.

11.2 Regional and Global Context

Bangladesh's approach to government blockchain builds upon international experience while addressing the specific requirements of its legal and institutional context. The Policy draws lessons from:

- India's National Blockchain Framework providing reference for sovereign, state-controlled blockchain infrastructure serving government applications at scale.
- China's Blockchain-based Service Network demonstrating approaches to balancing innovation enablement with regulatory control through permissioned models.
- Singapore's TradeTrust framework illustrating blockchain applications for international trade documentation with legal interoperability.
- The European Blockchain Services Infrastructure (EBSI) providing guidance on W3C standard adoption, GDPR-compliant architectures, and cross-border credential verification.

Through successful implementation, Bangladesh can emerge as a regional leader in government blockchain adoption, sharing experience through South-South cooperation and contributing to international standards development.

11.3 Critical Success Factors

Achieving the vision of this Policy requires sustained attention to several critical success factors:

Leadership Commitment: Continued high-level political and administrative commitment to blockchain adoption ensures resource allocation, inter-agency coordination, and priority attention to implementation challenges.

Institutional Capacity: Building and retaining skilled human resources across government and the broader ecosystem is essential for successful implementation and sustainable operations.

Stakeholder Engagement: Meaningful engagement with citizens, private sector, academia, and civil society ensures that blockchain initiatives address real needs and build broad support.

Adaptive Implementation: Technology and context evolve rapidly. Implementation approaches must be adaptive, learning from pilots and early deployments to refine subsequent phases.

Coordination Excellence: Blockchain initiatives span multiple agencies and require effective coordination mechanisms. The governance structures established in this Policy must function effectively in practice.

11.4 Call to Action

This Policy calls upon all stakeholders to contribute to successful blockchain adoption:

Government Agencies: Implementing ministries and agencies are called upon to establish blockchain focal points, engage actively in implementation planning, and embrace the change management required for blockchain-enabled service transformation.

Private Sector: Technology companies, consultancies, and service providers are encouraged to develop blockchain capabilities, participate in the regulatory sandbox, and partner with government on implementation.

Academic Institutions: Universities and research institutions are invited to integrate blockchain into curricula, conduct relevant research, and contribute to the knowledge base supporting implementation.

Civil Society: Civil society organizations are encouraged to engage constructively in policy dialogue, monitor implementation, and advocate for citizen interests in blockchain deployment.

Citizens: Citizens are encouraged to utilize blockchain-enabled services, provide feedback on service quality, and engage with digital literacy programs preparing them for credential wallet usage.

11.7 Closing Statement

Blockchain technology offers transformative potential for enhancing trust, transparency, and efficiency in government operations and citizen services. Through this National Blockchain Policy, Bangladesh establishes a thoughtful, comprehensive framework for realizing this potential while safeguarding citizen privacy, ensuring cybersecurity, and maintaining regulatory alignment.

The Policy recognizes that blockchain is not a solution to all challenges, but rather a powerful tool that, when applied appropriately within a sound governance framework, can contribute significantly to national development objectives. Success requires sustained commitment, adaptive implementation, and collaborative effort across government, private sector, academia, and civil society.

With this Policy as foundation, Bangladesh embarks on a journey toward blockchain-enabled digital transformation, building upon the legal frameworks of 2025 to create government services that are more transparent, more efficient, and more trustworthy. The journey begins with careful foundations and ambitious aspirations, guided by the principles of data sovereignty, privacy by design, and citizen empowerment that define Bangladesh's digital future.

DOCUMENT INFORMATION

Document Title	National Blockchain Policy of Bangladesh
Version	1.0
Date	2026
Issuing Authority	Information and Communication Technology Division, Ministry of Posts, Telecommunications and Information Technology
Policy Period	2026-2030
Review Cycle	Three years or as necessitated by significant developments