INSTITUTIONAL BLOCKCHAIN PROTOCOL

NABD

A technical overview for partners and operators

AT THE LAB | UNITED ARAB EMIRATES

DOCUMENT INDEX

CONTENTS

WHAT NABD IS

NABD is a permissioned blockchain protocol built for institutions that need deterministic finality, cryptographic agility, and sovereign control over their ledger. It is not a general-purpose public chain. It is designed for consortium networks, national infrastructure, and regulated financial settlement where trust boundaries are known but must still be enforced by the protocol.

The name comes from the Arabic word for pulse — the idea that consensus should be a living, measurable heartbeat across validators, not a probabilistic guess.

WHY IT MATTERS

Most institutional blockchains force a choice: fast but trusted, or slow and adversarial. NABD offers both modes in the same protocol, selectable at deployment time.

- **Private mode** optimizes for liveness among known validators — ideal for banks, regulators, and sovereign consortia.
- **Public mode** adds Byzantine hardening through VRF leader selection and strict message validation — for less trusted or externally visible validator sets.

Both modes share the same ledger model, transaction format, and governance path, so a network can start conservatively and evolve without a ledger migration.

For stablecoin and regulated-payment networks, privacy is not optional. Issuers, banks, merchants, and treasury desks need final settlement without exposing every counterparty relationship, payment route, or operational balance to a public explorer. NABD supports visible settlement assurance for operators while allowing private payment views where sensitive transfer fields are redacted.

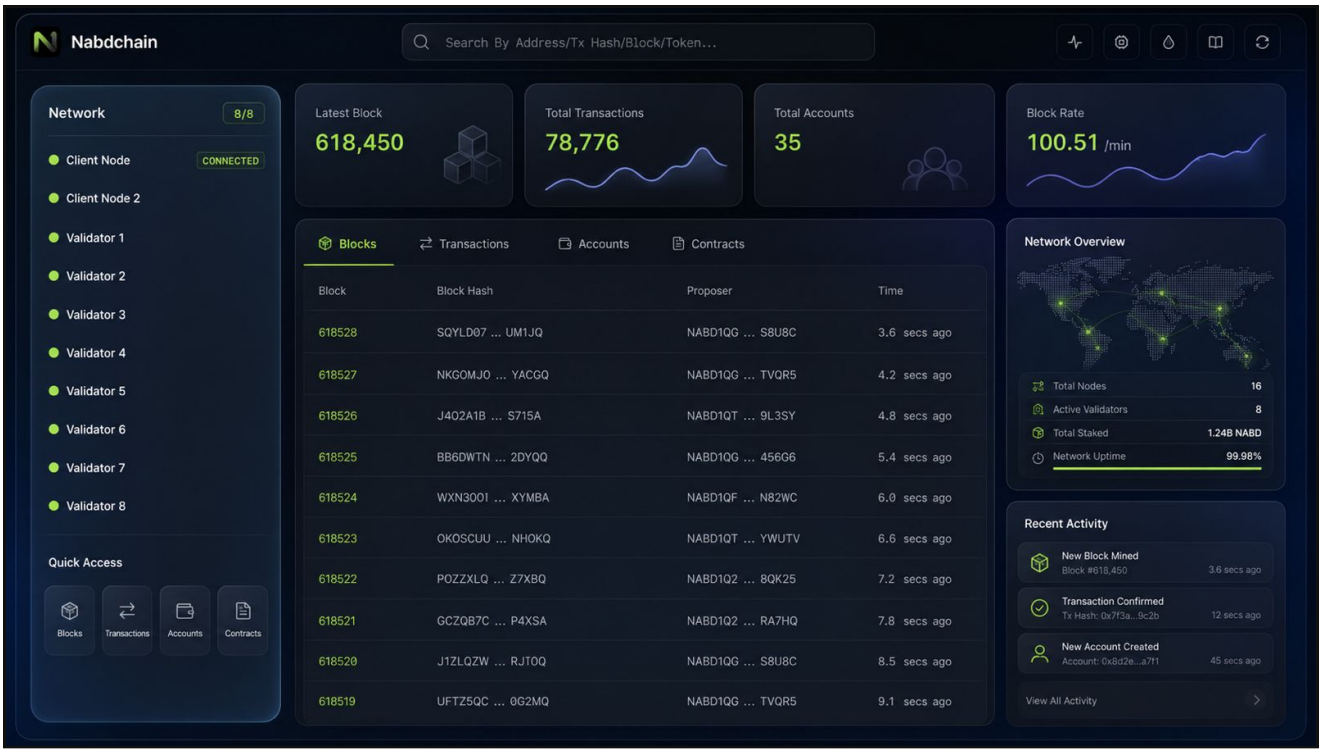
SPEED, FINALITY, AND PRIVACY

NABD is designed around deterministic finality. Once a transaction reaches the COMMIT phase with validator quorum, it is confirmed; operators do not wait for probabilistic block depth or multiple confirmation windows. That property matters for payment systems because a confirmed transfer can be treated as settled by applications, treasury workflows, and downstream reconciliation.

The private deployment profile optimizes for low-latency operation across known validators. The reference explorer interface below brings validator status, blocks, accounts, contracts, and transaction activity into one view. The same finality model applies to normal payments and private payments.

Privacy-preserving payments keep the network auditable without making every business relationship public. A private stablecoin transfer can retain transaction status, block height, timestamp, fee policy, and validator-verifiable settlement while redacting sender, recipient, and value fields from public-facing views.

CHAIN IN ACTION



NABD network and transaction activity in one explorer interface.

CORE DESIGN

1. Hybrid Post-Quantum Signatures

NABD supports three authentication modes natively: Ed25519 for current production, Falcon-512 for post-quantum policy domains, and a hybrid Ed25519+Falcon envelope for migration windows. The signature scheme is independent of the transaction payload, so changing cryptographic policy does not rewrite business logic.

2. Dual-Mode Consensus (NabdBFT)

Consensus runs in four phases — PROPOSE, VOTE, CERTIFY, COMMIT — with deterministic finality. Private mode uses round-robin leadership for predictable recovery. Public mode replaces that with verifiable-random-function selection to resist targeted leader disruption. Quorum is strictly Q = floor(2N/3) + 1 in both modes.

3. On-Chain Governance

Validator-set changes are not configuration edits. They are consortium_update transactions approved by the current validator quorum and activated at a bounded future round. This removes the need for offline coordination during membership changes.

4. Chain-Bound Transactions

Every transaction can carry network_id and genesis_hash fields. When enabled, validators reject transactions that do not belong to the running network. This eliminates replay risk across testnets, sidechains, or disaster-recovery forks.

5. Privacy-Aware Payment Rails

Private payment support lets operators choose what is visible to explorers and downstream systems. This is especially important for stablecoins, where the network must prove that settlement happened while protecting commercially sensitive transfer metadata.

DEPLOYMENT PROFILES

NABD is launched from reproducible profiles that encode node roles, consensus geometry, and operational expectations — not just validator counts.

PROFILE	VALIDATORS	QUORUM	USE CASE
Foundation-5	5	4	Pilot / private consortium
Resilient-7	7	5	Production consortium baseline
Scale-9	9	7	Higher traffic + API/archive redundancy

BAAS LAYER

NABD includes a Blockchain-as-a-Service control plane for operators who need repeatable deployment rather than manual node configuration. The control plane handles topology generation, key custody references, infrastructure provisioning, rolling

upgrades, health monitoring, and audit logging. It does not replace security review or key ceremonies, but it removes the operational drift that causes most production incidents.

For questions or partnership discussions: contact@atl.ae