

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

House Bill No. **5402**



Introduced by Representative
LEODY F. TARRIELA

EXPLANATORY NOTE

The Filipino people deserve a government where every peso is traced, verified, and accounted for — from the moment Congress appropriates it to the time it reaches the last constituency or beneficiary.

In today's digital economy, **trust and transparency** are no longer philosophical ideals; they are technological realities. The advent of **blockchain and distributed ledger systems** has redefined how nations safeguard public trust. These systems allow immutable, time-stamped records that cannot be altered without collective verification—transforming how we manage budgets, contracts, and audits.

The **National Distributed Budget and Governance Blockchain Act of 2025** seeks to institutionalize a unified digital ledger across all branches of public finance—from **appropriation to disbursement, procurement to audit**—powered by blockchain technology.

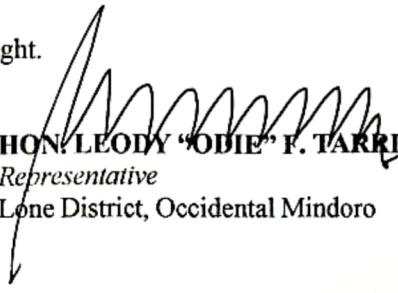
It mandates the establishment of a **National Budget Distributed Ledger (NBDL)** and a **Blockchain Budget Governance Board (BBGB)** composed of the **DICT, DBM, COA, DOF**, and independent auditors and competent private sectors. Through **Digital Public Assets (DPAs)**, every appropriation, SARO, NCA, and disbursement can be cryptographically linked and publicly verifiable—ensuring that no transaction escapes audit trail or citizen oversight.

This measure also introduces the concept of **Smart-Contract Modules (SCMs)**—automated release conditions that ensure funds are only disbursed upon verified milestones. With **phased rollouts and sandbox environments**, the law encourages responsible adoption, balancing innovation with fiscal prudence. The bill further empowers **local governments** to integrate into the NBDL network, enabling traceable fund transfers and transparent project execution at the grassroots level—while maintaining compliance with existing audit and procurement laws.

Beyond technology, this is about restoring confidence in governance. It operationalizes President Ferdinand Marcos Jr.'s directive for **digital transformation and transparency**, aligns with the **Department of Budget and Management's** ongoing blockchain pilot for public financial management, and positions the Philippines as a regional leader in **GovTech** innovation.

In an era where corruption thrives in opacity, the Filipino people demand verifiable accountability. This bill turns that demand into code.

Approval of this measure is earnestly sought.


HON. LEODY "ODIE" F. TARRIELA
Representative
Lone District, Occidental Mindoro

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

House Bill No. **5402**

INTRODUCED BY REPRESENTATIVE
LEODY F. TARRIELA

AN ACT

**Institutionalizing the National Distributed Budget and Governance
Blockchain System, Establishing the Blockchain Budget
Governance Board, and for Other Purposes**

*Be it enacted by the Senate and House of Representatives of the Philippines in Congress
assembled:*

SECTION 0. ACRONYMS AND TERMS (LEGEND).

BBGB	Blockchain Budget Governance Board
BTr	Bureau of the Treasury
COA	Commission on Audit
DBM	Department of Budget and Management
DICT	Department of Information and Communications Technology
DPA	Digital Public Asset
DOF	Department of Finance
GAA	General Appropriations Act
LGU	Local Government Unit
NBDL	National Budget Distributed Ledger
PO	Purchase Order
RA 9184	Government Procurement Reform Act
SARO / NCA	Special Allotment Release Order / Notice of Cash Allocation
SCM	Smart-Contract Module
Sandbox	Regulatory Sandbox under DICT-DBM-COA
Validator Node	Authorized node participating in consensus

SECTION 1. SHORT TITLE.

This Act shall be known as the “National Distributed Budget and Governance Blockchain Act of 2025.”

SECTION 2. DECLARATION OF POLICY.

It is hereby declared the policy of the State to promote good governance through transparency, accountability, and efficiency in public financial management. The State recognizes that emerging technologies such as blockchain and distributed ledger systems enable secure, immutable, and verifiable records for the life cycle of public funds. Accordingly, the government shall adopt these technologies to ensure traceability from appropriation to disbursement and audit through the adoption of blockchain in public financial management.

SECTION 3. SCOPE AND COVERAGE

This Act shall cover the entire national budget life cycle including appropriations, allotments, procurements, disbursements, and audits. It shall apply to all national government agencies, and shall be phased for LGU participation in later stages.

1. This act covers the Full National Budget Life Cycle
 - a) Preparation and legislative appropriation
 - b) Allotments and release orders
 - c) Procurement contracts, bidding, purchase orders
 - d) Disbursements and cash transfers
 - e) Project execution (reporting, milestones, deliverables)
 - f) Audit, reconciliation, supplemental/reprogramming
2. Key agencies:
 - a. Department of Budget & Management (DBM),
 - b. Department of Information and Communications Technology (DICT),
 - c. Commission on Audit (COA),
 - d. Department of Finance (DOF) — shall coordinate to implement this Act.
3. Local government units (LGUs) may opt into a compatible “Local Ledger Node” scheme under DOF/DBM guidelines in later phases.
4. This Act does not replace ordinary fiduciary rules, procurement laws (RA 9184 et al.), or audit rules; it augments them with a cryptographic audit trail.

SECTION 4. ESTABLISHMENT OF THE NATIONAL BUDGET DISTRIBUTED LEDGER (NBDL).

There is hereby created a National Budget Distributed Ledger (NBDL) that shall record all transactions involving public funds. The DICT shall serve as technical lead in coordination with DBM, COA, and DOF. A Blockchain Budget Governance Board (BBGB) is hereby constituted to set standards, approve system updates, and ensure data integrity.

Each agency shall operate an authorized Validator Node and issue Digital Public Assets (DPAs) corresponding to appropriations, allotments, or disbursements. Smart-Contract Modules (SCMs) may automate conditional releases based on verified milestones.

1. Institutional Roles & Governance.

a) DICT shall serve as the technical lead, in coordination with DBM and COA, to program, oversee, and maintain the NBDL infrastructure.

b) A "Blockchain Budget Governance Board (BBGB)" is hereby created, composed of representatives from DICT, DBM, COA, DOF, a civil society technical advisory panel, and an independent auditor.

c) The BBGB sets cryptographic, architectural, and policy standards (consensus rules, keys, on-chain/off-chain mapping).

2. Node Network & Validation.

a) Each major department (top 10), DBM, COA, DOF, and designated auditors shall operate validator or mirror nodes.

b) The network shall use a permissioned or hybrid consensus model optimized for performance, auditability, and fault tolerance.

3. DPA Issuance & Linking.

a) Upon appropriation, DBM shall issue Appropriation DPAs on the ledger, tagged with identifiers, metadata (program, line item, object code).

b) All subsequent obligations (allotments, PO, contracts, disbursements) must be timestamped and cryptographically linked to prior DPAs.

4. Smart Contract Modules.

a) Budget release may be mediated via Release Modules programmed with conditional logic (e.g. "release tranche when milestone verified by COA node").

b) Disbursement modules may trigger alerts or hold funds upon exceptions or mismatches.

5. Interoperability & Off-chain Systems.

a) The NBDL must expose APIs / proof interfaces to DBM eBudget, COA audit systems, procurement portals, Bureau of Treasury, etc.

b) For large volume transactions or gas constraints, off-chain batch anchors (Merkle roots) with proof paths may be accepted, provided auditors / stakeholders can verify.

6. Regulatory Sandbox & Phased Rollout.

a) The first stage (Year 1–2): Pilot deployment on 3–5 major national line agencies (e.g. DPWH, DOH, DEP-Ed).

b) Year 3–4: Expand to all national agencies, integrate reprogramming, supplemental DPAs.

c) Year 5: LGU integration, cross-agency linking, citizen interface, further features.

SECTION 5. BLOCKCHAIN BUDGET GOVERNANCE BOARD (BBGB).

A Blockchain Budget Governance Board (BBGB) is hereby created to oversee the standards, implementation, and continuous development of the National Budget Distributed Ledger (NBDL).

The Board shall be composed of:

- The Secretary of the Department of Information and Communications Technology (DICT) – Chairperson;
- The Secretary of the Department of Budget and Management (DBM) – Co-Chairperson;
- The Chairperson of the Commission on Audit (COA) – Member;
- The Secretary of the Department of Finance (DOF) – Member;
- One (1) representative from the academe with recognized expertise in distributed systems or financial governance – Member; and
- Two (2) representatives from the private sector, to be appointed by the BBGB from a shortlist submitted by the DICT and recognized industry associations, with proven competence in blockchain architecture, cybersecurity, fintech, or enterprise systems integration – Members.

The private-sector representatives shall serve without compensation, except for per diems and allowances as may be authorized by the Board, and shall hold office for a term of three (3) years, subject to renewal based on performance and continued good standing.

The BBGB shall:

1. Formulate and adopt national technical standards and interoperability frameworks for blockchain in government;
2. Approve protocols for cryptographic key management, data integrity, and node operations;
3. Oversee certification of validators and smart-contract modules; and
4. Recommend policy updates to Congress every two (2) years through the Committees on ICT and Appropriations.

SECTION 6. DIGITAL PUBLIC ASSETS (DPA).

All appropriations, allotments, and disbursements shall be represented as DPAs, each cryptographically linked to the source appropriation for traceability.

(a) All appropriations, allotments, obligations, and disbursements authorized under the General Appropriations Act (GAA), including special and supplemental funds, shall be issued, recorded, and tracked as Digital Public Assets (DPAs) within the National Budget Distributed Ledger (NBDL).

Each DPA shall represent a cryptographic tokenized record of a specific budgetary transaction, containing metadata such as:

1. Agency, program, project, or activity (PPA) code;
2. Object of expenditure and fund source (e.g., GAA item, special fund, foreign-assisted fund);
3. Authorized amount and unique DPA identifier;
4. Date and time of issuance and movement between entities (from DBM → implementing agency → contractor or LGU);
5. Purpose, output, or milestone to which the DPA is linked; and
6. Status flags for obligated, released, disbursed, or audited states.

(b) Each DPA shall be cryptographically linked to its originating appropriation through a verifiable chain of hashes, thereby establishing an immutable lineage of public funds from the original budget item to the final expenditure or liquidation.

(c) Transfers or utilization of DPAs shall require dual or multi-signature validation by authorized entities such as the DBM, COA, and the receiving agency. These validations shall be recorded as on-chain events, producing a tamper-proof audit trail accessible to oversight bodies.

(d) The BBGB shall issue technical and data standards to ensure interoperability between the NBDL and existing government systems, including but not limited to:

- DBM's eBudget and eAppropriations System;
- COA's Audit Tracking and Verification Systems; and
- DOF/BTr's Treasury Single Account (TSA) architecture.

DPAs shall be structured to integrate with these systems via secure APIs and off-chain proofs for performance efficiency.

(e) No DPA shall be deemed valid unless it bears a digital signature generated by a recognized Validator Node, as registered with the Blockchain Budget Governance Board (BBGB).

Unauthorized creation, duplication, alteration, or deletion of DPAs shall constitute tampering of public records and cybercrime, punishable under Republic Act No. 10175 (Cybercrime Prevention Act of 2012), without prejudice to administrative and criminal liability under existing laws.

(f) For public transparency, the NBDL shall maintain a read-only public interface displaying non-sensitive information such as project title, location, implementing agency, amount released, and project status, allowing citizens to verify the flow of funds in real time.

SECTION 7. AUDIT, MONITORING AND PUBLIC ACCESS.

COA shall run Validator Nodes for real-time verification and maintain a public, read-only ledger interface. The COA shall use its own Validator Node for real-time audit verification.

A public read-only Budget Ledger Explorer shall be maintained to allow citizens to verify transactions without revealing sensitive personal data. Independent cryptographic audits shall be conducted annually.

1. On-chain audit & public dashboard.

a) A publicly accessible "Budget Ledger Explorer" shall be provided, enabling citizens to inspect DPAs, transactions, and proofs (read-only).

b) COA node(s) must verify each block; any irregularities shall result in immediate alerts to oversight committees.

2. Third-party audit & red teaming.

a) The BBGB shall invite external cryptographic audit firms (domestic or international) to conduct security, privacy, and compliance audits annually.

b) A “Bug Bounty / Audit Reward Fund” shall be established to incentivize ethical disclosure.

3. Exception handling & reversals.

a) If an irregular transaction is found malicious, a Dispute Module enables a controlled roll-back or freeze (within agreed policy constraints) only under COA + BBGB authority.

b) Formal notices and reports must be filed in both NBDL and conventional audit channels.

SECTION 8. SUPPLEMENTAL AND EMERGENCY ALLOCATIONS.

Any reprogramming, supplemental budget, or budget realignment must issue Supplemental DPAs linked to original appropriations, recording reason, authority, and timestamp. Emergency releases (e.g. calamities, pandemics) may bypass standard modules, but must still be logged with explanatory metadata, subject to COA review.

SECTION 9. KEY CUSTODY AND SECURITY.

The BBGB shall implement cryptographic key management, multisignature control, and hardware security measures.

1. The BBGB shall define a Key Management Policy, including multi-signature custody, hardware security modules, threshold schemes, periodic rotation, and emergency recovery.
2. Cryptographic standards shall follow recognized public norms (e.g. SHA-256, ECC) and updates in consultation with DICT / cybersecurity agencies.
3. Access control, identity management, and role assignments must align with existing civil service and fiduciary rules.
4. All code modules, smart logic, and infrastructure must undergo independent security review before deployment in production.

SECTION 10. APPROPRIATIONS AND FUNDING.

1. The initial implementation (pilot phase) shall be funded from the DBM’s Digital Transformation Fund (or equivalent).
2. Subsequent funding shall be included in the General Appropriations Act (GAA) as a line item for “NBDL Operations and Maintenance.”
3. The BBGB may accept grants, donations, or technical assistance (local or foreign) subject to full disclosure and COA oversight.

SECTION 11. IMPLEMENTING RULES AND REGULATIONS. (IRR)

Within ninety (90) days after the effectivity of this Act, DICT, DBM, COA, DOF, and the BBGB shall jointly promulgate the IRR, including detailed technical standards, transition plan, node accreditation, audit procedures, a Business Continuity Plan for Public Governance as a structured framework that ensures uninterrupted delivery of essential government functions and public services during and after any form of disruption — whether caused by natural calamities, cyberattacks, pandemics, political instability, or technological breakdowns, disaster recovery, and national security measures.

SECTION 12. PENALTIES AND SANCTIONS.

- (a) Any person, whether natural or juridical, who willfully and unlawfully interferes with, manipulates, or compromises any component of the National Budget Distributed Ledger (NBDL), including but not limited to the creation, modification, or deletion of Digital Public Assets (DPAs), shall be liable under the following provisions:

1. Unauthorized Access and Hacking.

Any act of accessing, intruding, or attempting to penetrate the NBDL or Validator Nodes without authority shall be punishable under Sections 4(a)(1) and 4(a)(5) of Republic Act No. 10175 (Cybercrime Prevention Act of 2012), with penalties of imprisonment of six (6) years and one (1) day to twelve (12) years and/or a fine of up to Five Hundred Thousand Pesos (P500,000) for each count, without prejudice to higher penalties under related laws.

2. Tampering or Forging of DPAs.

Any person who intentionally alters, duplicates, forges, or fabricates DPAs, hashes, or cryptographic proofs to misrepresent the flow of public funds shall, in addition to the penalties under the Cybercrime Prevention Act, be liable under the Revised Penal Code (Articles 171–172, Falsification of Public Documents) and corresponding anti-graft statutes such as Republic Act No. 3019 (Anti-Graft and Corrupt Practices Act) and Republic Act No. 6713 (Code of Conduct and Ethical Standards for Public Officials and Employees).

3. Unauthorized Key Generation or Use.

Any public official or authorized contractor who generates, distributes, or uses cryptographic keys, signatures, or Validator credentials outside approved BBGB policies shall suffer penalties of imprisonment of four (4) years and one (1) day to eight (8) years, disqualification from public office, and forfeiture of benefits. The Blockchain Budget Governance Board (BBGB) shall immediately refer such violations to the Department of Justice (DOJ) and the Cybercrime Investigation and Coordinating Center (CICC) for prosecution.

4. Negligent Oversight or Reckless Handling.

Public officials who, by gross negligence or reckless inaction, allow a breach, data compromise, or unauthorized transaction resulting in public fund loss shall be held administratively liable under the Civil Service Commission (CSC) and Commission on Audit (COA) rules, and may be suspended or dismissed from service after due process.

5. Private Contractors and Technical Service Providers.

(a) Any private-sector entity or technical provider found complicit in tampering, manipulation, or obstruction of the NBDL shall be blacklisted from all government contracts for a minimum of five (5) years, in addition to criminal prosecution under existing laws.

(b) The imposition of penalties under this section shall be without prejudice to civil liability, restitution of public funds, or recovery of damages by the State.

(c) In all cases, the COA, CSC, BBGB, and other relevant agencies shall coordinate with the National Bureau of Investigation (NBI) and CICC for evidence preservation, digital forensics, and prosecution support.

(d) The BBGB shall promulgate within ninety (90) days from the effectivity of this Act the Guidelines on Accountability and Incident Response outlining classification of violations, procedures for forensic investigation, and coordinated enforcement protocols with relevant law-enforcement bodies.

SECTION 13. SEPARABILITY CLAUSE.

Invalidity of any provision shall not affect the remainder of this Act.

SECTION 14. REPEALING CLAUSE.

All inconsistent laws are hereby repealed or modified accordingly.

SECTION 15. EFFECTIVITY.

This Act shall take effect fifteen (15) days after publication in the Official Gazette or in two (2) national newspapers of general circulation.