Position Paper in Support of the “Blockchain the Budget Bill” (Senate Bill No. 1330)
Written by: ENGR. OSCAR P. OGANIZA, Founder TechTribe Media, Co-Founder Ginhawa

Introduction

As someone deeply involved in local government system development and digital governance initiatives, I have observed how limitations in transparency and control create opportunities for the misuse of public funds.

Manual processes, discretionary approvals, and fragmented systems make it difficult to trace accountability and ensure that every peso is properly spent. These weaknesses, while often overlooked, reveal how outdated systems can unintentionally enable inefficiency and corruption.

The proposed Blockchain the Budget Bill (SB 1330) provides a significant step toward restoring public trust and promoting good governance. I fully support this initiative and offer the following technical and governance insights for its implementation, particularly in the area of procurement and infrastructure management.

However, based on my professional experience, blockchain alone functions primarily as a ledger of transactions — an immutable record of “what happened.” While it strengthens audit trails, it does not inherently prevent corruption unless combined with AI-driven validation, smart contracts, and automated enforcement mechanisms.

For blockchain to make a real impact in public governance, it must be designed as part of a decision-enforcing ecosystem, not merely a passive record-keeping tool.

Observations

No.	Observation / Process Area	Actual Corruption Situation Observed	Description / Analysis	Recommendation	Involved Office(s)	Mechanism to Stop Corruption
1	**Discretionary Powers in Bids and Awards Committee (BAC)**	Bid results are pre-arranged or influenced by personal interests.	Discretionary powers within the BAC allow manipulation of scoring and bid approvals.	Replace human discretion with AI-assisted bid evaluation and store all decisions in a blockchain audit ledger.	DTI, COA, GPPB, DICT – ensure removal of human discretion in evaluation and awards.	Bid evaluation parameters (e.g., price, compliance score) are encoded in Smart Contracts. AI ranks all bids automatically, and the Smart Contract releases award data only after all criteria are satisfied and cryptographically verified.
2	**Changes Between Purchase Request (PR) and Purchase Order (PO)**	Amounts and quantities altered without traceability.	Manual editing enables manipulation and overpricing.	Require immutable blockchain logging for all PR–PO revisions.	Budget Office, Accounting, Procurement, DICT – enforce AI rule-based validation of changes.	Any overage or quantity change is automatically rejected unless a higher authority cryptographically signs a Budget Amendment on-chain.
3	**Ghost Beneficiaries**	Fake or duplicate beneficiaries listed in aid programs.	Lack of identity verification enables fraudulent entries.	Integrate PhilSys-based D-ID verification for all aid disbursements.	DSWD, NEDA, DICT, PSA – adopt automated digital ID verification.	Funds are locked in Smart Contracts and released only to PhilSys-verified D-ID wallets. Final cash-out requires biometric Proof-of-Receipt, ensuring a live, verified individual receives the aid.
4	**Static Contract Systems**	Contractors exploit static pricing for inflated adjustments.	Contracts not linked to real-time pricing data.	Use Dynamic Smart Contracts that adjust automatically to verified market indices.	DPWH, DTI, DBM, DICT – automate contract price recalibration.	Contract values are auto-linked to DTI's verified market indices. If material costs exceed thresholds, the Smart Contract triggers a Price Review Request requiring cryptographic approval before release.
5	**Unjustified Infrastructure Change Orders**	Change orders approved without technical validation.	No data-driven standard for evaluating revisions.	Create AI-Blockchain Expert System to analyze and approve change orders.	DPWH, COA, DICT – automate change order validation.	AI algorithms evaluate proposed changes using project baselines and engineering data.

						Smart Contract rejects any unverified change order, unless digitally signed by a licensed engineer and validated on-chain.
6	**Ghost Deliveries**	Deliveries recorded as complete without actual goods received.	Manual sign-offs enable falsified deliveries.	Adopt IoT-integrated Smart Contracts that confirm delivery before payment.	Procurement, COA, DICT, DILG, Logistics – automate delivery verification.	GPS, QR, and IoT sensors verify actual delivery data. The Smart Contract releases payment only upon verified Proof-of-Delivery, ensuring the physical item reached its intended recipient.
7	**Receipt and Payment Documentation**	Audits influenced by personal relations or pre-arranged reviews.	Manual review creates room for manipulation.	Deploy AI-powered, blockchain-backed audit verification and AI-randomized auditor selection.	COA, DBM, DICT, Treasury Office – eliminate human discretion in audit routing.	Auditors are selected through AI randomization, and audit approval workflows are locked in Smart Contracts. No payment can be finalized without on-chain dual verification by two independent, randomly assigned auditors.
8	**Blank or Fabricated Receipts**	Some offices use pre-signed or blank receipts to justify liquidations or add arbitrary amounts to access funds.	The lack of digital receipt validation allows manual encoding of unverified transactions. These are often used to inflate expenses or liquidate funds without proof of actual purchase.	Require Digital Receipts generated only from registered suppliers under a DTI-verified Smart Billing System, automatically linked to procurement and accounting modules.	COA, DTI, DBM, Treasury Office, DICT – eliminate manual liquidation entries and ensure AI validation of receipt authenticity.	Receipts are issued and signed digitally through a blockchain-registered DTI merchant system. The Smart Contract validates receipt authenticity, and funds are released only after the merchant's digital signature and tax record are verified on-chain. Any "blank" or unverified receipt is automatically rejected by the system.

9	**Transactions Without Official Receipts (e.g., Confidential and Intelligence Funds)**	Certain transactions, such as those classified under “Confidential” or “Intelligence” funds, are legally permitted to operate without standard receipts or detailed liquidation. This creates opportunities for untraceable disbursements and inflated claims.	While the Constitution allows confidentiality for specific security-related expenditures, the lack of receipt-based documentation can be exploited for personal or political gain. It weakens financial traceability and removes accountability mechanisms present in other government funds.	Implement a blockchain-based encrypted ledger for confidential transactions, allowing recording of fund movements without disclosing sensitive details. Each entry should include digital signatures, time-stamps, and classification tags accessible only to authorized oversight bodies (COA, DBM, or Senate Committees).	COA / DBM / Office of the President – Remove full discretionary approval; confidential fund transactions should still be cryptographically logged under restricted visibility to ensure oversight integrity.	Each confidential transaction is recorded in an encrypted blockchain ledger visible only to authorized oversight bodies. Smart Contracts ensure that fund disbursement aligns strictly with predefined confidential expenditure policies. Any unverified or duplicate disbursement attempt is automatically blocked, and all movements require a cryptographic audit trail for post-event verification.

Note

Corruption in government operations is not merely a technical flaw — it is a human problem enabled by discretionary powers, weak accountability, and manual systems. Technology gives us the chance to change that.

To those working in government, I know that many of you understand these realities. You may not be corrupt — but some among your staff might be. I have personally witnessed how easily the system can be abused from the inside. This is why it is essential to design systems that remove discretion, automate decisions, and encode accountability directly into the digital process.

The current Full Disclosure Policy (FDP), while well-intentioned, is not truly transparent. What is often disclosed to the public are summarized or post-processed figures, not real-time, verifiable transactions. This lack of granular data visibility is itself a reflection of how corruption survives — hidden beneath compliance checklists and selectively published reports. When the information disclosed comes from the same people who may manipulate it, the policy loses its integrity.

I strongly believe that the proposed Blockchain the Budget Bill (SB 1330) should go beyond simply recording data on a blockchain. Blockchain is only a ledger — it captures what happened, but it cannot prevent what shouldn't happen unless paired with AI validation, IoT verification, and smart contracts that enforce rules automatically.

Let us not stop at blockchain alone. Let us integrate all possible technologies — from digital identity verification, real-time analytics, automated audits, and AI-powered oversight — to finally end the culture of corruption that has weakened public trust for decades.

Governance should not depend on who is honest. It should depend on how well the system is built to make dishonesty impossible. Only then can transparency become real, measurable, and incorruptible.

This position paper was written with the assistance of Artificial Intelligence (AI), but all concepts, insights, and recommendations reflect the personal understanding and perspective of Oscar Oganiza.