

BD-VoteNet: A Fully Decentralised, Tamper-Proof Electronic Voting System for Bangladesh and Its Diaspora

Version 4.0 — Comprehensive Technical White Paper

Omar Marosh, CTO, Jionex Technologies

Date Issued: 1 August 2025

INTRODUCTION

In an era where blockchains move more value every 24 hours than most nations print in a year, our ballots still too often depend on *opaque boxes and blind trust*. The **dissonance** is staggering. As digital citizens we sign billion-dollar smart contracts from a phone, yet as voters we queue in the heat hoping a paper trail isn't lost in a back room. This inequity is no longer acceptable. Today's cryptographic tools can make fraud mathematically impossible, tampering instantly visible, and participation as easy as a tap—but only if we, the people, demand it.

BD-VoteNet stands on the shoulders of the same decentralized technologies that secures trillions of dollars daily across Bitcoin, Ethereum and other public chains. It distills those breakthroughs into one **uncompromising promise**: every voice counted, every count provable, no excuses.

In 2025, anything less is a **betrayal of basic democratic rights**. The blueprint you hold is not just a Bangladeshi project; it is a manifesto for every nation whose citizens believe that legitimacy must be earned in the open, verified by code and sealed by cryptographic truth.

We invite technologists, lawmakers and everyday voters alike: do not settle for whispers of fairness—demand proofs. Expect nothing short of radical transparency. Claim the democracy your century can deliver.

Table of Contents

1. Executive Summary
 2. Context & Motivation
 3. Design Principles & Guarantees
 4. System Architecture Overview
 5. Networking & Consensus
 6. Security Analysis
 7. Mathematical Foundations of Tamper-Proofness
 8. Physical Implementation & Hardware Tamper-Proofing
 9. Blockchain System Internals
 10. Governance & Legal Framework
 11. Risks & Open Questions
 12. Conclusion
 13. Key References
-

1 Executive Summary

BD-VoteNet delivers cryptographic certainty, universal accessibility and total transparency to every Bangladeshi voter—whether residing in Dhaka or Dubai, Khulna or Kansas. The platform fuses decentralised identity (BD PASS), threshold cryptography, zero-knowledge proofs (ZKPs) and a permissioned Byzantine-fault-tolerant (BFT) blockchain to eliminate single points of failure, ensure that only eligible citizens can vote *once*, and enable anyone to verify the final tally without compromising ballot secrecy.

2 Context & Motivation

- EVM trust deficit: Bangladesh's electronic voting machines were suspended after concerns over transparency and vendor lock-in.
 - Diaspora disenfranchisement: Roughly 13 million expatriates rarely manage to vote.
 - Global convergence: Nations such as Switzerland and Estonia are moving toward end-to-end-verifiable, open-source election systems.
 - Mobile readiness: With >180 million mobile subscriptions in 2024, even remote unions possess intermittent coverage, enabling a leapfrog to secure digital voting.
-

3 Design Principles & Guarantees

#	Principle	Guarantee	Core Mechanisms
1	Decentralisation	No single actor can alter votes or the voter roll.	HotStuff-based BFT blockchain with 15 core validators (Election Commission, Supreme Court IT Cell, BUET, CUET, two NGOs, two diaspora councils) plus $\geq 3\,000$ rural edge relays.
2	Tamper-Proof Voter Eligibility	Only legitimate citizens may vote, and only once.	Multi-party-computed voter roll $\rightarrow$ Merkle-tree commitment $\rightarrow$ zero-knowledge membership proofs $\rightarrow$ single-use voting tokens.
3	End-to-End Verifiability	Any voter can prove a ballot was recorded as <i>cast</i> and tallied as <i>recorded</i> .	Cast-as-intended encrypted ballot, on-chain publication, homomorphic tally, public Groth16 proof of correct decryption.
4	Anonymity with Accountability	Ballots unlinkable to identities; double-voting impossible.	ElGamal/Paillier encryption, verifiable shuffle (Neff), credential-balanced unlinkable signatures.
5	Universal Accessibility	Every voter—including those offline, low-literacy or abroad—can participate.	Android/iOS/Web apps, embassy kiosks, solar edge nodes, QR “vote-capsules,” LoRa/SMS fallback, Bengali + English + Arabic UI with text-to-speech.

4 System Architecture Overview

4.1 Layers

1. Core Validator Layer
 - 15 validator clusters reach HotStuff consensus and maintain the canonical ledger.
 - Each cluster houses dual 1U servers, redundant NICs, mirrored SSD arrays and a YubiHSM-2 pair.
2. District Relay Layer (64 nodes)
 - Mini-PCs with TPMs cache recent blocks, serve RPC queries and bridge edge traffic to validators.
3. Rural Edge Layer (≈3 000 nodes)
 - Raspberry Pi 5 + OPTIGA TPM, solar panel, LTE/LoRa radio.
 - Provide offline ballot ingestion, local receipt printing, and store-and-forward to relays.
4. Client Layer
 - Mobile app, web app and kiosk UI share the same open-source codebase.
 - Support screen-reader mode, audio prompts and low-bandwidth asset bundles.
5. Audit Layer
 - A read-only explorer renders every block, Merkle proof and ZKP for public inspection.

5 Networking & Consensus

- Transport: libp2p + QUIC; gossip scoring prevents eclipse attacks.
- Consensus: HotStuff with a 4 s view-change; $n = 3f + 1$, $f = 5$.
- Latency: Core-to-core commit <2 s; edge batch-sync every 5–30 min depending on link quality.
- Leader Election: Reputation-weighted round-robin; misbehaviour slashes on-chain score and rotates leader immediately.
- Sybil Protection: Validator identity keys anchored in e-gov PKI, HSM-backed and audit-logged.

6 Security Analysis

Threat	Mitigation
Voter-roll tampering	MPC computation by multiple parties; Merkle root published on-chain + print; discrepancy aborts election.
Ballot stuffing	Voting token is single-use; smart contract rejects duplicates.
Double voting	Same token cannot be reused; earliest block wins; duplicate logged.
Ballot secrecy breach	Mixnet with Neff shuffle + DDH-secure ElGamal; privacy reduction $< 2^{-128}$.
Coercion / vote-selling	Receipt reveals no choice; panic-ballot feature allows cast override.
Edge node compromise	Cannot decrypt ballots; any invalid ZKP rejected by validators.
Consensus break	<i>HotStuff safety theorem:</i> In a system of $n = 3f + 1$ replicas, no two honest replicas ever commit different blocks at the same height as long as at most f replicas are Byzantine—regardless of network delays.
DoS on rural voters	LoRa mesh, SMS chunking and sneaker-net ensure submission; backlog cached.
Quantum attacks	Hybrid ECDSA/Dilithium signatures; ballot ciphertext destroyed after tally.

7 Mathematical Foundations of Tamper-Proofness

7.1 Notation

- $H(x)$ = SHA-3-256 hash
- $E_{pk}(m; r)$ = ElGamal encryption of message m with randomness r
- $\llbracket m \rrbracket$ = Paillier ciphertext of m
- Π_{range} = ZK range proof asserting vote $\in \{c_1, \dots, c_M\}$
- $\Pi_{shuffle}$ = Verifiable shuffle proof per Neff

7.2 Integrity of the Voter Roll

Each leaf $\ell_i = H(NID_i \parallel constituency_i \parallel epochID)$. Root R is written to block 0. Collision-resistance $\Rightarrow$ any modified roll yields $R' \neq R$, detectable by comparing printed and on-chain roots (probability of undetected tamper $\leq 2^{-128}$).

7.3 Uniqueness of Ballots

Let $spent[tokenID]$ be a Boolean in the on-chain state. Smart-contract transition:

if $spent[tokenID] == \text{true}$: reject

else: $spent[tokenID] \leftarrow \text{true}$; accept

Because state is finalised by HotStuff after 2 rounds, a second transaction with the same $tokenID$ is rejected unless $\geq 1/3$ validators equivocate (contradicts safety theorem).

7.4 Ballot Privacy & Unlinkability

Ciphertexts are re-encrypted and shuffled; $\Pi_{shuffle}$ proves permutation correctness without revealing mapping. Breaking unlinkability reduces to solving DDH in secp256k1; advantage negligible for $\lambda = 128$.

7.5 Correctness of the Tally

Paillier is additively homomorphic: $\llbracket m_1 \rrbracket \cdot \llbracket m_2 \rrbracket = \llbracket m_1 + m_2 \rrbracket$. Validators compute the product of all ballots $\Rightarrow$ encrypted sum. Threshold decryption (t-of-n) produces a plaintext sum. Groth16 circuit validates:

1. All Π_{range} proofs valid.
2. Decryption shares pass pairwise-consistency checks.
3. Output commitment equals encrypted sum.
Knowledge-soundness of Groth16 $\Rightarrow$ tally sound with probability $\geq 1 - 2^{-128}$.

7.6 Consensus Safety & Liveness

Safety Theorem: No two honest validators commit conflicting blocks if $\leq f$ validators are Byzantine.

Liveness Theorem: Under partial synchrony, an honest leader's proposal eventually commits.

(Proofs identical to Yin et al., 2019, §§4–5.)

7.7 Parameter Choices

Primitive	Parameter	Security Bits
Hash	SHA-3-256	128 (collision) / 256 (pre-image)
Paillier	4 096-bit	128
ElGamal	secp256k1	128
ZKP	Groth16 over BLS12-381	128
Threshold	$t = n - f$ ($\geq \frac{2}{3}$ honest)	—

8 Physical Implementation & Hardware Tamper-Proofing

8.1 Kiosk Bill-of-Materials

Module	Specification	Justification
Compute	Rockchip RK3588 SBC, 8 GB RAM	Runs ZKP verification offline.
Display	13" IPS, 400 nits	Sunlight readability.
Authentication	CMOS fingerprint reader + 2 D barcode scanner	Biometric fallback; BD PASS QR scan.
Secure Element	TPM 2.0 on I ² C + measured boot	Cryptographic root of trust.
Connectivity	LTE Cat-6, Wi-Fi 5, LoRa 125 kHz	Redundancy + rural reach.
Power	50 W mono-crystalline panel + 100 Wh LiFePO ₄	12 h off-grid runtime.
Printer	58 mm thermal	Optional voter-verifiable paper audit trail.
Tamper Sensors	Reed-switch, accelerometer, case-open microswitch	Wipes TPM EK if breached.

8.2 Validator Rack

- Dual Xeon Silver, 64 GB ECC, mirrored SSD, redundant PSU
- YubiHSM-2 cluster (2 of 3 threshold)
- Remote attestation via Intel TXT + TPM quote; monitored by Prometheus

8.3 Rural Edge Node

- Raspberry Pi 5, Infineon OPTIGA TPM
- 40 W flexible PV panel + 50 Wh LiFePO₄ + PoE fallback
- LTE/LoRa gateway; pushes batched ballots every 10-30 min

8.4 Tamper-Proofing Measures

- Secure Boot (UEFI → GRUB → dm-verity).
 - Epoxy-potted flash & TPM.
 - Conformal-coated boards with mesh wiring; cut/short triggers zeroise.
 - Regular remote-attestation heartbeat; stale nodes quarantined.
-

9 Blockchain System Internals

9.1 Ledger Objects

Object	Key Fields	Purpose
BlockHeader	parentHash, height, stateRoot, voteRoot, rollRoot, timestamp, proposerSig	Anchors all on-chain state.
VoteTx	tokenID, ciphertext, Π _range, voterSig	Records a single encrypted ballot.
RollDeltaTx	leafHash, courtOrderID, multiSig	Court-ordered voter-roll additions/removals.
TallyTx	cipherTotal, shares[], Π _tally	Posts final homomorphic tally + ZKP.

9.2 State-Transition Phases

Phase	Accepts	Rejects	Exit Condition
Init	RollDeltaTx VoteTx x		pollOpenTime reached.
Open	VoteTx	Duplicate tokenID; further RollDeltaTx	pollCloseTime reached.
Close	—	New VoteTx	TallyTx posted and verified.
Final	—	Any mutating tx	Chain frozen.

9.3 Throughput & Storage

- VoteTx size: ≈ 2 kB (ciphertext + ZK).
- Block size: 2 MB $\rightarrow \sim 1\,000$ tx.
- Burst throughput: 1 000 tx/s (parallel cores).
- Full electorate (120 M voters): 240 GB total; IPFS multi-pin + erasure coding; offline snapshots stored on LTO-9.

10 Governance & Legal Framework

1. Voter-Roll Oversight Board: EC, Supreme Court, ruling/opposition IT delegates, two civil-society orgs. Decisions require $\frac{2}{3}$ multi-signature.
2. Validator Charter: Public SLAs; cryptographic misbehaviour triggers automatic slashing and legal liability.
3. Open-Source Licence: GPL-3; source, build scripts, formal proofs public on multi-mirrored Git Servers with SSL, publicly available hashes for source-code, source-builds; bounty programme for bugs.
4. Regulatory Alignment: Operates in RPO §91B sandbox; draft amendments prepared for 2027 parliamentary passage.

11 Risks & Open Questions

Category	Risk	Mitigation
Digital Divide	Elderly/rural distrust of digital	Maintain paper trail, nationwide voter-education drive, radio/TV explainers.
Validator Cartel	Collusion among validators	Cap per-entity stake; on-chain slashing; randomised leader rotation; external auditors.
Legislative Delay	RPO amendments stall	Pilot evidence + bipartisan oversight board.
Supply-Chain	Firmware implants	Reproducible builds, open hardware designs, third-party side-channel tests.
Quantum Threat	Future decryption	Hybrid PQ signatures now; swap to lattice schemes before 2030.

12 Conclusion

BD-VoteNet 4.0 unifies cryptographic rigor, resilient hardware and transparent governance to deliver elections that are hacker-proof, fraud-proof and tamper-proof while remaining inclusive for every Bangladeshi citizen worldwide. With open-source verifiability and an incremental rollout plan, Bangladesh can set a new global benchmark for electoral trust.

This is by no means a final static solution, but rather a framework to plan for the future. We present what is currently cutting edge technology with our limited expertise.

But, by presenting this white-paper and inviting the public to share in the vision, and to contribute to the project would make it as robust as has been proven by countless massive open-source projects that are resilient, successful and scalable.

13 Key References

1. Yin, M. et al. *HotStuff: BFT Consensus in the LAN and in the WAN*. IEEE S&P 2019.
2. Khan, A. et al. *A Secure End-to-End Verifiable E-Voting System Using Blockchain*. 2021.
3. Islam, R. et al. *Zero-Knowledge Proof-Based EVS Design*. *Journal of Cyber-Security*, 2025.
4. Swiss Post. *E-Voting Technical Documentation*. 2024.
5. Springer Survey. *Blockchain for Securing Electronic Voting Systems*. 2024.
6. The Daily Star. *People's Loss of Faith in Elections*. 2023.
Cost & Infrastructure Estimate (Phase-1 Pilot)
| Item | Qty | Unit USD | Sub-Total |

Disclaimer:

ChatGPT Model o3 has been used to ideate and research many parts of this project.

Jisan and I began this idea on the eve of the ex Prime Minister's ousting, Shaikh Hasina on 5th August 2024. Almost 1 year ago. We began by thinking about how we can build an Electronic Voting system for Bangladesh that is tamper-proof and decentralized. We looked at many technologies available to us, and worked through various challenges that we would face in an environment such as Bangladesh where not only the population is vast, but dispersed, many remote and many without access to mobility and internet connectivity.

We looked at decentralized internet connectivity, radio based mesh networking, and others. All those ideas still hold in case of a possibility that communications itself is no longer a trusted commodity in a country that seeks fair elections.

And our idea evolved to thinking about tamper-proofness, trust of voter call, bipartisan trust, and proving that the code that runs the machines has not been tampered with.

We do believe that the technology that is available to us today, put in a framework to address these problems has the ability to run such a grandiose vision of a fair election. This white paper is only a start toward that vision. We publish it today, to start the awareness campaign and to document what is possible and what we, at Jionex hope to build with and for the people of Bangladesh.