

Security Analysis and Hardened VRF-Reputation PBFT for Distributed Medical Diagnostic Consensus

Haewon Byeon

Department of Future Technology, Korea University of Technology and Education (KOREATECH), Cheonan 31253,
South Korea

Abstract—Distributed intelligent medical diagnostic systems require consensus mechanisms that remain efficient while preventing malicious or low-quality diagnostic agents from shaping the ledgered clinical decision process. A recent VS-PBFT algorithm combines a verifiable random function (VRF) with dynamic reputation to improve practical Byzantine fault tolerance in medical diagnostic collaboration. This study performs an anchor-paper-centered security analysis of VS-PBFT rather than proposing a generic consensus variant. The protocol is reconstructed from its published equations and pseudocode, and four weaknesses are examined: byte-truncation modulo bias in leader election, ambiguity in the persistent binding between VRF public keys and node identities, reputation accumulation by protocol-valid but semantically harmful votes, and the absence of an explicit epoch-stable quorum rule when low-reputation nodes are excluded. A hardened variant, HVS-PBFT, is proposed with hash-to-range leader mapping, certified persistent VRF keys, dual-component reputation, on-off behavior penalties, and epoch-bound membership with quorum recalculation. Safe proof-of-concept validation is performed using symbolic attack traces, bounded state simulation, Monte Carlo security experiments, event injection, local cryptographic microbenchmarks, and statistical tests. Under the tested conditions, the original byte-mapping rule at 40 nodes exhibits a 16.67% relative theoretical election advantage for favored indices, while HVS-PBFT reduces harmful-commit rates in the modeled collusion scenario at the cost of approximately 8 ms additional consensus latency. The results support a bounded security-performance trade-off, not an unconditional proof of security.

Keywords—PBFT; verifiable random function; reputation mechanism; blockchain consensus; healthcare security; safe POC; Byzantine fault tolerance

I. INTRODUCTION

Permissioned blockchain systems are increasingly used to coordinate data integrity, auditability, and multi-party decision-making in healthcare networks. Their practical value is strongest when several institutions, medical data centers, or diagnostic agents must agree on a record without placing all trust in a single central server. Liu et al. proposed VS-PBFT for this setting by combining VRF-based master-node selection with dynamic reputation in a distributed intelligent medical diagnostic collaboration system [1]. The anchor protocol seeks to improve PBFT scalability and reduce malicious node interference while preserving deterministic consensus properties derived from the PBFT lineage [2], [3].

This study does not treat the anchor article as a background citation only. It uses the published message logic, equations, and algorithms as the object of cryptanalytic and experimental evaluation. That choice is important because recent PBFT variants often report lower latency or reduced communication overhead, yet the leader-selection, reputation, and membership mechanisms that create those gains can introduce new security assumptions [4]-[13]. A reputation-weighted consensus algorithm can become fragile if a syntactically valid message is rewarded even when its semantic effect is harmful. A randomized leader-election mechanism can become biased if a short random fragment is mapped to a node set by a nonuniform modulo operation. A dynamic exclusion rule can also disturb PBFT fault thresholds if the active committee is changed without an epoch-level quorum calculation.

The anchor protocol is attractive as a target because it provides enough detail to reconstruct a concrete election and reputation mechanism. Algorithm 2 computes a candidate leader using $r[0] \bmod N$, where $r[0]$ is the first byte of the generated VRF output. Algorithm 3 rewards message validation largely through signature, client-match, and view-number checks. The study also states that nodes below a reputation threshold are excluded from consensus. These features make the study suitable for safe proof-of-concept validation: no external system is attacked, no credential is stolen, and no denial-of-service tool is deployed. Instead, the protocol is tested through symbolic state models, Monte Carlo leader-election trials, synthetic collusion events, and statistical evaluation.

The contribution of this study is fourfold. First, it reconstructs the VS-PBFT election and reputation core and separates confirmed findings from specification ambiguities. Second, it shows that byte truncation followed by modulo mapping creates measurable leader-selection bias when N does not divide 256. Third, it proposes HVS-PBFT, a conservative hardening of VS-PBFT that preserves the VRF-reputation architecture while binding VRF keys to identities, using unbiased hash-to-range selection, splitting reputation into security and diagnostic components, and freezing membership at epoch boundaries. Fourth, it reports safe POC results under explicit assumptions and interprets them as bounded evidence rather than operational certification. The dependencies among randomness, reputation, membership, and quorum decisions are illustrated in Fig. 1.

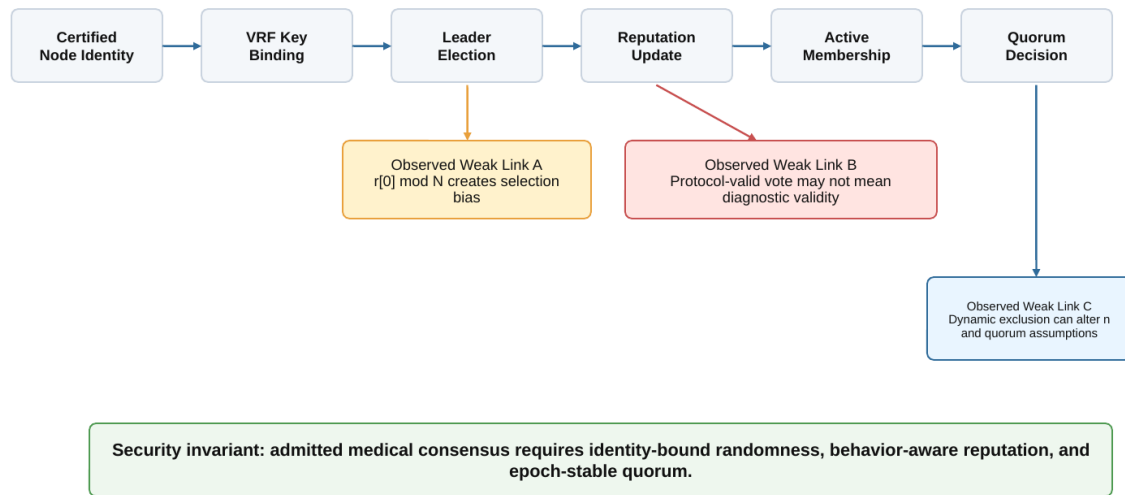


Fig. 1. Consensus security dependency map linking identity-bound randomness, reputation, active membership, and quorum decisions.

II. RELATED WORK

PBFT remains a foundational protocol for permissioned and consortium blockchains because it gives deterministic finality under a bounded Byzantine adversary. Classical PBFT tolerates f faulty replicas among n replicas when $n \geq 3f + 1$, but its all-to-all communication cost becomes restrictive as n grows [2], [3]. This has motivated grouped, hierarchical, low-storage, and reputation-assisted variants. ULS-PBFT reduces storage overhead by reorganizing the consensus structure [4]. SG-PBFT uses score grouping for intelligent Internet of Vehicles environments [5]. R-PBFT introduces an intelligent reputation-based design for vehicular consensus [6]. Healthcare-oriented PBFT work has similarly used feature trust and VRF-style primary selection to lower communication cost while preserving a permissioned trust model [7].

Several PBFT variants select smaller or higher-quality committees. P-PBFT supports pharmaceutical traceability with an improved consensus process [8]. Xie et al. modeled primary-node election as a probabilistic linguistic decision problem [9], while genetic selection, hierarchical mesh-and-spoke models, and two-stage trust-reward architectures have also been used to reduce consensus delay and communication overhead [10]–[12]. S-PBFT uses clustering and two-layer consensus for microgrid trading [13]. These studies support the general direction of VS-PBFT but also show why node selection and reputation updates must be audited as security mechanisms, not merely as performance optimizations.

Reputation systems are useful because they transform observed behavior into a persistent decision signal, but they have well-known attack surfaces. Surveys of reputation systems describe ballot stuffing, bad-mouthing, collusion, whitewashing, and on-off behavior as recurring concerns [14], [15]. Machine-learning security studies similarly show that systems trained or updated from adversarial behavior can be manipulated through poisoning, evasion, and non-independent data patterns [16], [17]. In a medical diagnostic consensus system, this lesson is directly relevant: a vote may be cryptographically valid and still be clinically harmful or strategically coordinated.

VRF-based randomness can reduce predictability in leader selection, but the implementation details matter. FortunChain demonstrates how EC-VRF can support scalable blockchain sharding [18], and distributed reputation systems for peer-to-peer energy trading show how fairness must be handled when trust scores shape participation [19]. Healthcare blockchain reviews emphasize auditability, access control, data integrity, and interoperability as the main reasons for using blockchain in health information systems [20]–[24]. Broader blockchain reviews also stress that consensus choice imposes trade-offs among throughput, decentralization, energy cost, finality, and security [25]–[28]. This study positions HVS-PBFT within that trade-off space.

TABLE I. CANDIDATE WEAKNESSES AND HARDENING MECHANISMS

Finding	Status	Main evidence	HVS-PBFT response
Modulo-biased leader mapping	Confirmed for $r[0] \bmod N$	Algorithmic mapping uses one byte before modulo	Hash-to-range with rejection sampling
VRF key identity ambiguity	Conditional	View-change pseudocode regenerates a key pair	Certified NodeID VRF_pk epoch binding
Protocol-valid harmful votes	Conditional	Reputation verification checks syntactic validity	Dual security/diagnostic reputation
Dynamic exclusion vs quorum	Conditional	Nodes under threshold are excluded	Epoch-bound active set and $q_e = 2f_e + 1$
On-off reputation gaming	Modeled risk	Attackers can farm reputation during honest periods	Decay, behavior-change penalty, quarantine

III. SYSTEM AND THREAT MODEL

The modeled system contains a trusted authority, medical AI diagnostic agents, a medical data center, patient-side request channels, and a permissioned blockchain consensus layer. The trusted authority handles identity authentication, key distribution, and reputation assessment in the anchor design. The medical diagnostic model supplies candidate outputs, and the consensus mechanism confirms the accepted diagnostic result. The key dependency is circular: diagnostic outputs affect consensus votes, consensus behavior updates reputation, and reputation influences future participation. This loop is useful

only if the reputation score measures both protocol compliance and the quality of the diagnostic action.

The adversary is a bounded active network and insider adversary. It can observe, delay, reorder, and replay protocol messages in a synthetic network model; corrupt a subset of diagnostic agents; coordinate colluding votes; and inject malformed or malicious-but-syntactically-valid behavior into the simulator. It cannot break Ed25519 unforgeability, invert cryptographic hash functions, compromise every trusted-authority share, or attack real clinical systems. The safe POC deliberately models DoS and collusion as arrival processes and state variables rather than live traffic against any external target.

The security properties tested are fairness of leader selection, persistent identity-to-election-key binding, resistance to reputation capture, membership stability, and bounded liveness under malicious-node ratios. Confidentiality of patient records and transport encryption are not the main objects of this study. They remain important for deployment, but the anchor protocol already assumes TLS, PKI, AES-256, and blockchain-EHR middleware. The present analysis focuses on whether the consensus-specific security mechanisms support their own claims when they interact.

IV. RECONSTRUCTION OF THE VS-PBFT CORE

The anchor protocol introduces VRF selection and dynamic reputation into PBFT. Each node has a reputation value R_i initialized at 50. A node below a specified threshold is excluded from the consensus process. In simplified notation, the published reputation rule can be reconstructed as $R_i = R_i + k \cdot T - m \cdot F$ with $0 < R_i < 100$. A later concrete update uses a small increase for successful participation and a penalty for failure, approximately $R_i \leftarrow R_i + 0.09$ for success and $R_i \leftarrow R_i - 0.5$ for failure. Algorithm 3 admits participation only when $R_i > 30$ and then checks message conditions such as signature validity, client matching, and view numbering.

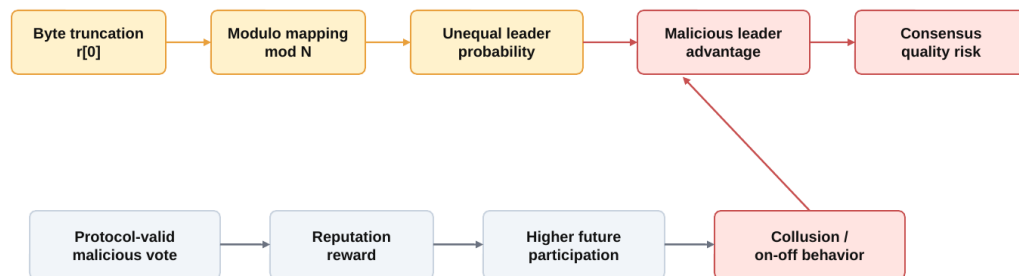


Fig. 2. Bias and reputation-manipulation attack propagation in the VS-PBFT election and reputation loop.

B. VRF Identity Binding Ambiguity

The second finding is a high-probability specification weakness rather than a confirmed implementation attack. The view-change pseudocode contains $(pk, sk) \leftarrow G(\lambda)$ inside the leader-election routine. If read literally, a node may generate a fresh VRF key during view change. That would make it unclear how validators bind the proof to a pre-certified node identity, role, membership epoch, and reputation record. The safe trace is: A node enters view v_prime , uses a VRF key not previously bound to its NodeID, broadcasts $BV(v_prime, LN, pi, r)$, and validators verify the proof but not the persistent

The leader-election routine is reconstructed as follows. Given the current view v , total node count N , and current leader L , the protocol sets $v_prime = v + 1$ and $SD = \text{"leader-election"} \parallel v_prime$. The pseudocode then generates a key pair, obtains a proof $pi = CP(sk, SD)$, computes a random output $r = CO(pi)$, and calculates $CL = r[0] \bmod N$. If CL equals the previous leader, the algorithm uses $LN = (CL + 1) \bmod N$; otherwise, $LN = CL$. The resulting leader information is broadcast with the new view, proof, and random output.

The anchor article states general VRF properties of verifiability, uniqueness, and pseudorandomness. It also describes a custom random-output process built from SHA-512, weighted exponentiation, logarithmic and product terms, XOR, and SHA-256. Because this study focuses on consensus-level safety rather than low-level cryptanalysis of Ed25519 or SHA-512, the custom VRF-like procedure is not declared broken. The confirmed weakness concerns the election mapping after random generation. Even a perfectly random byte becomes a biased selector when mapped by modulo to a set size that does not divide the byte space.

V. VULNERABILITY ANALYSIS

A. Confirmed Modulo Bias in Leader Selection

The first finding is confirmed by arithmetic and simulation. In the anchor election rule, $Leader = r[0] \bmod N$. For $N = 40$, the byte space has 256 values and $256 = 40 \cdot 6 + 16$. Therefore, leader indices 0 through 15 receive seven byte values each, while indices 16 through 39 receive six byte values each. The probabilities are $7/256$ and $6/256$, producing a relative advantage of 16.67% for the favored indices. This is not a full leader-control attack, but it weakens the fairness claim and increases the chance that node identifiers assigned to favored residues receive more proposals over long runs. The propagation path is shown in Fig. 2.

election credential. The violated property is accountable leader eligibility. This finding remains conditional because implementation code may use persistent keys even if the pseudocode is imprecise.

C. Reputation Accumulation by Protocol-Valid Harmful Behavior

The third finding concerns semantic validity. In Algorithm 3, the successful validation predicate is reconstructed as $SV \text{ AND } CM \text{ AND } VIM$, where SV denotes signature validity, CM denotes client matching, and VIM denotes view-number

matching. A malicious diagnostic agent can therefore be syntactically valid while submitting a harmful, biased, or collusive diagnostic vote. The symbolic trace is: Node i signs a valid PREPARE/READY message; the message matches the client and view; $\text{Verify}(m_i) = \text{Accept}$; reputation increases; the diagnostic content is not independently penalized in the consensus-side rule. The violated property is not cryptographic authentication, but behavior-faithful reputation. This is a critical distinction. VS-PBFT can authenticate who voted while still rewarding a vote that should lower trust in the clinical decision process.

D. Dynamic Exclusion and Quorum Instability

The fourth finding concerns PBFT membership. When reputation falls below the threshold, a node is excluded from consensus. If membership changes immediately while a consensus instance is active, the active node count n_{active} and Byzantine bound f_{active} may no longer match the quorum used by replicas. The safe trace is: some nodes are excluded after reputation changes; honest replicas calculate quorum with different active sets or stale assumptions; a Byzantine coalition exploits the mismatch to create liveness failure or to increase its voting share. The property at risk is epoch agreement on membership and quorum, not the original PBFT proof under a fixed membership. The identified weaknesses and corresponding hardening mechanisms are summarized in Table I.

VI. HARDENED HVS-PBFT DESIGN

HVS-PBFT keeps the original purpose of VS-PBFT: efficient medical diagnostic consensus using PBFT, VRF selection, and reputation. It changes only the mechanisms that create the identified risks. The first change replaces one-byte modulo mapping with hash-to-range leader selection. The algorithm expands the VRF output to a fixed-length digest and maps it with rejection sampling or a standard unbiased range-reduction method. For $N = 40$, a one-byte example would reject

values from 240 to 255; a practical implementation should use at least 64 bits so that rejection probability becomes negligible for ordinary committee sizes.

The second change is a certified election credential. At registration, the trusted authority or threshold authority signs $\text{Cert}_i = \text{Sign_TA}(\text{NodeID}_i \parallel \text{VRF_pk}_i \parallel \text{Role}_i \parallel \text{membership_epoch} \parallel \text{expiry})$. A node may not use a new VRF key in a view change unless the new key appears in a fresh certificate. This preserves the unpredictability of VRF output while making the winner accountable. A proof verifies both the VRF relation and the authority-certified binding between the public key and the node that owns the reputation record.

The third change separates reputation into security and diagnostic components. R_{security} is updated by protocol events such as valid signatures, equivocation, double voting, stale view use, malformed proof, and replay. $R_{\text{diagnostic}}$ is updated by diagnostic-quality events, cross-validation, ground-truth feedback when available, and later audit evidence. The combined score can be written as $R_i = \alpha R_{\text{security}_i} + \beta R_{\text{diagnostic}_i}$, but HVS-PBFT prevents either component from dominating without an application-specific policy. This avoids treating a valid signature as evidence of a correct medical judgment.

The fourth change freezes membership within an epoch. At the beginning of epoch e , the active set Active_e is fixed and publicly committed by a signed membership digest. The protocol calculates $n_e = |\text{Active}_e|$, $f_e = \text{floor}((n_e - 1)/3)$, and $q_e = 2f_e + 1$. Reputation updates are still recorded during the epoch, but exclusion takes effect only at the next epoch boundary unless a separate emergency-suspension rule is triggered. If $n_e \geq 3f_e + 1$ is not satisfied for the current active set, the system does not force consensus; it enters a recovery or reconfiguration path. Fig. 3 summarizes the HVS-PBFT workflow.

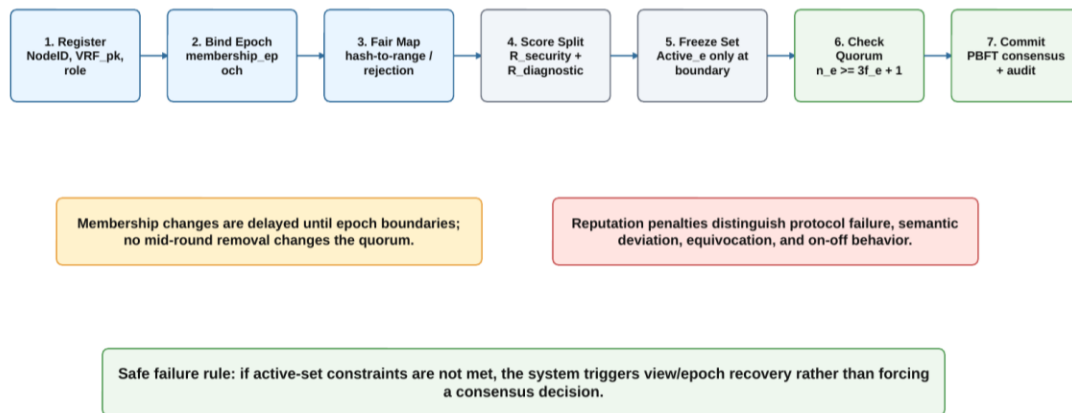


Fig. 3. HVS-PBFT epoch workflow with certified VRF keys, unbiased mapping, dual reputation, and explicit quorum calculation.

VII. SAFE POC METHODOLOGY AND RESULTS

The evaluation uses seven safe POC principles. No live hospital system, external blockchain, network target, or credential collection is used. The POC consists of symbolic attack traces, bounded protocol-state simulation, Monte Carlo leader-election trials, discrete-event performance modeling,

local cryptographic microbenchmarks, compromise/reputation event injection, and statistical validation. Table II lists the experimental design. The random seed was fixed at 20260902. Leader-election trials used 200,000 elections per node-size condition. Reputation simulations used 60 replicates, 100 rounds per replicate, and malicious-node ratios from 0 to 33%.

TABLE II. SAFE POC CONFIGURATION

POC type	Purpose	Implementation
Symbolic trace	Express attacker knowledge and verification paths	Manual state/event model
Bounded verification	Check epoch, quorum, membership invariants	Python bounded state simulation
Monte Carlo	Estimate election bias and reputation capture	200,000 election trials; 60 replicate security runs
Discrete event	Measure latency and consensus response	Synthetic processing and queue model
Microbenchmark	Estimate hash, HMAC, Ed25519 overhead	Local Python cryptography benchmark
Event injection	Inject collusion, on-off, malicious leader, membership change	Closed simulator only
Statistical validation	Test differences and uncertainty	Chi-square and Mann-Whitney U tests

The analytical and simulated fairness results agree. At $N = 40$, original VS-PBFT had maximum observed leader probability 0.027685 and minimum probability 0.022630 across 200,000 elections. Its chi-square statistic against the uniform distribution was 1195.09 with $p < 10^{-200}$. HVS-PBFT, using unbiased range reduction, reduced the maximum observed deviation. The remaining small deviation was sampling noise in a finite trial rather than a structural byte-mapping bias. The result confirms a fairness defect, but it does not imply that an outside attacker can choose the leader at will.

The reputation/collusion POC models protocol-valid malicious votes as syntactically acceptable in original VS-PBFT. Under $N = 40$ and a 30% malicious-node ratio, original VS-PBFT showed an average harmful-commit rate of 0.1578, while HVS-PBFT reduced the rate to 0.0278 under the same synthetic attack workload. The final malicious-node reputation remained high in the original model, averaging 58.37, because participation was often rewarded despite harmful semantic behavior. In HVS-PBFT, the final malicious reputation averaged 28.52 because diagnostic deviation, on-off behavior, and collusion events were penalized separately. Mann-Whitney

U tests comparing bad-commit rates favored HVS-PBFT in all tested malicious-node conditions at $N = 40, 80$, and 160.

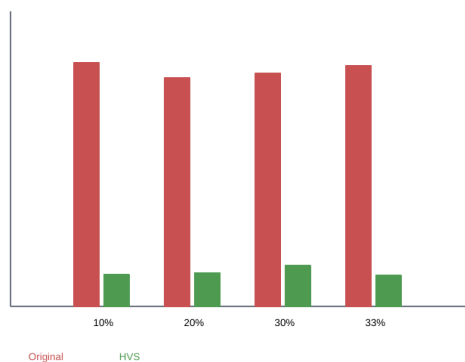
Performance changed in the expected direction. The strengthened design adds certificate checks, digest binding, event classification, and epoch logic. At $N = 40$ and a 30% malicious-node ratio, the synthetic consensus-latency model increased from about 81.0 ms to about 89.0 ms. The overhead is acceptable in the modeled setting because the security gain is tied to a clear reduction in harmful commits and reputation capture. A local microbenchmark showed mean costs of approximately 0.63 microseconds for SHA-512, 1.66 microseconds for HMAC-SHA256, 34.97 microseconds for Ed25519 signing, 106.62 microseconds for Ed25519 verification, and 0.95 microseconds for 64-bit hash-to-range mapping. These figures are hardware- and library-specific and should be treated only as local evidence that unbiased mapping is not a dominant cost.

To improve transparency of the experimental workflow, a representative closed-environment simulation screen is also provided (Fig. 4 and 5). Fig. 5 shows a bounded Safe POC execution log that summarizes the command used, the fairness calculation, the collusion and reputation simulation outputs, and the associated nonparametric significance tests.

TABLE III. SELECTED SAFE POC RESULTS

Metric	Original VS-PBFT	HVS-PBFT	Interpretation
$N=40$ leader probability range	0.022630-0.027685	0.023975-0.025905	Structural modulo bias reduced
$N=40$ chi-square p-value	$< 10^{-200}$	0.040	Original strongly nonuniform in finite test
Bad-commit rate, $N=40$, 30% malicious	0.1578	0.0278	Dual reputation reduces harmful acceptance
Final malicious reputation, same setting	58.37	28.52	HVS penalizes semantic and on-off behavior
Mean latency, same setting	81.0 ms	89.0 ms	Security adds bounded overhead
64-bit hash-to-range cost	Not used	0.95 us mean	Mapping overhead is small locally

Bad commit rate at 40 nodes



Leader-selection deviation

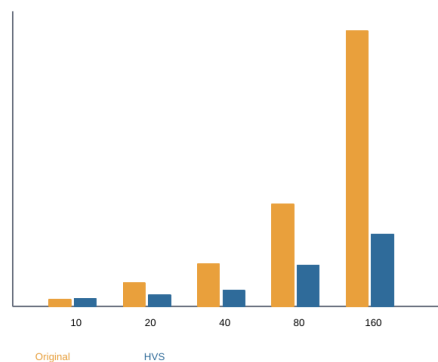


Fig. 4. Safe POC results comparing harmful commit rates and leader-selection deviation in original VS-PBFT and HVS-PBFT.

```
POC Simulation Log

$ python safe_poc_runner.py --seed 20260902 --nodes 40 --malicious 0.30
[INFO] Safe POC mode enabled: no external attack traffic generated
[INFO] Trials: fairness=200000, security replicates=60, rounds/replicate=100
[INFO] Running analytical fairness check for Original VS-PBFT and HVS-PBFT ...

Fairness N=40
method      max_prob  min_prob  max_dev_pct  chi_square  p_value
Original VS-PBFT  0.027685  0.022630  10.74        1195.0948   2.64e-225
HVS-PBFT      0.025905  0.023975  4.10         55.7308    4.01e-02

Security summary N=40, malicious_ratio=0.30
method      mal_leader  bad_commit  latency_ms  final_mal_rep
Original VS-PBFT  0.312333   0.157833   81.047      58.372
HVS-PBFT      0.228667   0.027833   89.002      28.525

Mann-Whitney U tests for bad-commit rate
mr=0.10  p=1.18e-21  mr=0.20  p=1.31e-21
mr=0.30  p=2.39e-21  mr=0.33  p=1.14e-21

[OK] Result: HVS-PBFT reduces biased selection and harmful commits
under the tested bounded conditions with modest latency overhead.
```

Fig. 5. Representative Safe POC simulation screenshot showing the closed, non-invasive execution log used for fairness analysis, collusion-event injection, and statistical testing.

VIII. DISCUSSION AND LIMITATIONS

The strongest confirmed result is the modulo-bias finding. It is mathematical, reproducible, and directly tied to the published election equation. The reputation findings are more conditional because the published paper contains a high-level medical system description and the repository states that the intelligent medical diagnosis model is conceptual rather than fully implemented. Therefore, this manuscript classifies protocol-valid harmful voting, identity-binding ambiguity, and dynamic-quorum instability as design weaknesses unless implementation-level evidence confirms the stronger interpretation. That conservative treatment is deliberate. A cryptanalysis paper loses credibility if it converts every ambiguity into a claimed exploit. Selected fairness, security, and performance results are summarized in Table III. Harmful-commit rates and leader-selection deviations are compared in Fig. 4.

HVS-PBFT should also be understood as a hardened research prototype. It improves the binding between randomness, identity, reputation, and membership, but it does not prove that a medical diagnostic model is clinically correct. A consensus mechanism can record agreement over a diagnostic output; it cannot decide whether the diagnostic model was properly validated, whether the input data are unbiased, or whether the final clinical action is appropriate. The proposed dual reputation mechanism therefore requires domain-specific validation data and governance rules. In deployments, `R_diagnostic` must be tied to clinical audit, model validation, or post-hoc outcome review rather than only to majority agreement.

The POC is safe and reproducible, but it is still a model. The latency values are generated by a discrete-event abstraction and local cryptographic timing, not by a full NS-3 execution or a multi-hospital blockchain deployment. The study did not execute ProVerif, Tamarin, Scyther, AVISPA, Docker, or

Kubernetes. Such tools can be added in a later phase, but this manuscript does not claim results that were not produced. The correct interpretation is narrower: under bounded symbolic and stochastic assumptions, HVS-PBFT reduces specific election and reputation risks introduced by the original combination of VRF and dynamic reputation.

The findings have broader implications for consensus design. Consensus optimizations often compress randomness, restrict committee size, or reward selected behaviors to improve throughput. Each optimization creates an additional security invariant. Randomness must remain unbiased after mapping. Reputation must measure adversarially relevant behavior. Membership must stay stable long enough for the quorum proof to remain meaningful. Healthcare systems add another layer: data integrity and auditability are necessary, but they do not automatically imply medical validity or regulatory sufficiency. HVS-PBFT is designed around those boundaries.

IX. CONCLUSION

This study analyzed VS-PBFT as an anchor protocol for distributed medical diagnostic consensus and identified one confirmed fairness defect and several conditional design weaknesses in the interaction between VRF selection, reputation, and membership management. The proposed HVS-PBFT design preserves the original PBFT-VRF-reputation architecture while adding unbiased leader mapping, certified persistent VRF keys, dual-component reputation, on-off penalties, and epoch-bound quorum recalculation. Safe POC experiments show that the hardened design reduces biased selection and harmful-commit rates under the modeled collusion conditions, with a modest latency cost. Future work should execute the model in NS-3 or a comparable testbed, validate diagnostic reputation against clinical-quality signals, and add formal verification models for epoch membership and correspondence properties.

FUNDING

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF-RS-2023-00237287, 2026S1A5A01004224).

DECLARATION ON GENERATIVE AI

Generative AI was used only to assist with language drafting and formatting. The author remains responsible for the study design, interpretation, verification of references, and final manuscript content.

REFERENCES

- [1] S. Liu, Y. Zhang, and Y. Zhao, "Consensus optimization algorithm for distributed intelligent medical diagnostic collaborative systems based on verifiable random functions and reputation mechanisms," *Electronics*, vol. 14, no. 10, Art. no. 2020, 2025.
- [2] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398-461, 2002.
- [3] W. Zhong, C. Hu, W. Xu, and J. Wang, "Byzantine fault-tolerant consensus algorithms: A survey," *Electronics*, vol. 12, no. 18, Art. no. 3801, 2023.
- [4] H. Luo, "ULS-PBFT: An ultra-low storage overhead PBFT consensus for blockchain," *Blockchain: Research and Applications*, vol. 4, no. 4, Art. no. 100155, 2023.
- [5] G. Xu, H. Bai, J. Xing, T. Luo, N. N. Xiong, X. Cheng, S. Liu, and X. Zheng, "SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 1-11, 2022.
- [6] A. Kumar, L. Vishwakarma, and D. Das, "R-PBFT: A secure and intelligent consensus algorithm for Internet of vehicles," *Vehicular Communications*, vol. 41, Art. no. 100609, 2023.
- [7] P. Hegde and P. K. R. Maddikunta, "Secure PBFT consensus-based lightweight blockchain for healthcare application," *Applied Sciences*, vol. 13, no. 6, Art. no. 3757, 2023.
- [8] S. Liu, R. Zhang, C. Liu, and D. Shi, "P-PBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability," *Computers in Biology and Medicine*, vol. 154, Art. no. 106590, 2023.
- [9] M. Xie, J. Liu, S. Chen, G. Xu, and M. Lin, "Primary node election based on probabilistic linguistic term set with confidence interval in the PBFT consensus mechanism for blockchain," *Complex & Intelligent Systems*, vol. 9, pp. 1507-1524, 2023.
- [10] J. Zhang, Y. Yang, D. Zhao, and Y. Wang, "A node selection algorithm with a genetic method based on PBFT in consortium blockchains," *Complex & Intelligent Systems*, vol. 9, pp. 3085-3105, 2023.
- [11] J. Li, Z. Li, F. Wang, and X. Chen, "MANDALA: A scalable blockchain model with mesh-and-spoke network and H-PBFT consensus algorithm," *Peer-to-Peer Networking and Applications*, vol. 16, pp. 226-244, 2023.
- [12] H. Qushtom, J. Misic, V. B. Misic, and X. Chang, "A two-stage PBFT architecture with trust and reward incentive mechanism," *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11440-11452, 2023.
- [13] Z. Yao, Y. Fang, H. Pan, X. Wang, and X. Si, "A secure and highly efficient blockchain PBFT consensus algorithm for microgrid power trading," *Scientific Reports*, vol. 14, Art. no. 8300, 2024.
- [14] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Computing Surveys*, vol. 42, no. 1, pp. 1-31, 2009.
- [15] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618-644, 2007.
- [16] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Srndic, P. Laskov, G. Giacinto, and F. Roli, "Evasion attacks against machine learning at test time," *Machine Learning*, vol. 92, pp. 387-402, 2013.
- [17] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," *Machine Learning*, vol. 81, no. 2, pp. 121-148, 2010.
- [18] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Applied Energy*, vol. 295, Art. no. 117056, 2021.
- [19] Q. Zhang, S. Wang, D. Zhang, J. Wang, and J. Sun, "FortunChain: EC-VRF-based scalable blockchain system for realizing state sharding," *IEEE Transactions on Network and Service Management*, vol. 20, no. 4, pp. 4340-4353, 2023.
- [20] M. Holbl, M. Kompara, A. Kamisalic, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, Art. no. 470, 2018.
- [21] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, Art. no. 56, 2019.
- [22] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *Journal of Medical Internet Research*, vol. 21, no. 2, Art. no. e12439, 2019.
- [23] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, W. A. Bukhari, and M. I. A. Khan, "Blockchain technology in healthcare: A systematic review," *PLOS ONE*, vol. 17, no. 4, Art. no. e0266462, 2022.
- [24] H. S. A. Fang, S. A. Tan, and M. Tan, "Blockchain personal health records: Systematic review," *Journal of Medical Internet Research*, vol. 23, no. 4, Art. no. e25094, 2021.
- [25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55-81, 2019.
- [26] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: A review and outlook," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719-6742, 2022.
- [27] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, Art. no. 47, 2022.
- [28] Y. Merrad, R. Amiri, M. Meghazi, and M. Cheriet, "Blockchain: Consensus algorithm key performance indicators, trade-offs, current trends, common drawbacks, and novel solution proposals," *Mathematics*, vol. 10, no. 15, Art. no. 2754, 2022.