Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

THE SEARCH OF A PRIVACY-PRESERVING AND COST-EFFECTIVE BLOCKCHAIN FRAMEWORK OF LARGE-SCALE E-VOTING

*

Pushkar Pandey
School of Computer Science and Engineering
,Galgotias University Gautam Budha Nagar,Uttar Pradesh
pushkarpandeyazm@gmail.com
Karan Bisht
School of Computer Science and Engineering
,Galgotias University Gautam Budha Nagar,Uttar Pradesh
karanbisht0095@gmail.com
Dr. Maneesh Upadhya
School of Computer Science and Engineering,
Galgotias University Gautam Buddha Nagar, Uttar Pradesh
maneesh.upadhya@galgotiasuniversity.edu.in

ABSTRACT

Historical and centralized electronic voting (e-voting) sys-tems have severe weaknesses in the areas of security, trans-parency and scalability that withhold the lack of public trust. Although they provide a solution to transparency, the first-generation blockchain-based models added severe new challenges concerning the aspects of scalability, cost, and privacy of ballots. Scalability, Privacy, Security, and Coercion-Resistance are the main research issues that have been contin-uously identified in the literature. The current paper suggests a new Hybrid-Layered, Privacy-Preserving Voting (HLPV) architecture, which meets all these challenges directly. HLPV architecture separates the system into two high-interoperability special registers: (1) a permissioned Authentication Ledger (AL) with Combinative Poor Byzantine Fault Tolerance con-sensus mechanism to provide high integrity voter registration, and (2) My Public high-throughput Tallying Ledger (TL), dropped on the Polygon sidechain to cast ballots at low cost and transparently and reliably. Paillier homomorphic encryp-tion helps the system to ensure a high level of ballot secrecy

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

and non-coercibility. Using this cryptography primitive, it is possible to have a completely public tallying on chain of all the encrypted ballots and still not decrypt any individual votes, which allows resolving the tension between verifiability and privacy. The HLPV model is shown to be quite efficient, inheriting the insignificant gas charges of Polygon and the low latency authentication of PBFT-based hybrid designs. It provides a direct answer to the main research difficulty through offering a broad-based solution, which is both scalable, private, auditable, and resistant to coercion.

I. INTRODUCTION

Voting is the central mechanism of the modern day democ-racy, and the procedures involved in the administration.it are still marred with inefficiencies and weaknesses that destroy public trust. Traditional paper based voting Systems are infa-mously slow, resource-consuming and non transparent. They are acutely vulgar to various malfunctions, such as a hu-man error in tallying, physical ballot abuse,[9],[12] logistical problems, including ”booth capture” or ”dummy voting” and stuffing of the ballot. The systems do not provide a voter with a way to confirm

that he or she has cast a ballot and the ballot was counted deliberately, weakening the validity of the outcomes. When the information era came, it was suggested that electronic voting (e-voting), including through, be centralized. One of the solutions is an Electronic Voting Machine (EVM) or Internet platform. However, these systems tend to just computerize the weaknesses trading physical in-security with digital insecurity. A centralized e-voting system creates a critical single point of failure: the central. server. This is a voter data storing and results tabulating server that is a high value target to attackers.an array of attacks, such as advanced malware, Distributed Denial of Service (DDoS).disenfranchisement attacks, malicious insider or state-level manipulation. actors. This black box method compels all the voters to put their complete faith in the invisible. Third party administrators, proprietary code as well as opaque hardware. This monopoly of power, along with a basic absence of transparency and verifiability, has resulted in a general popular.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

A. Problem Definition

Numerous existing and proposed e-voting designs are based on public Layer-1 .platforms, the most popular of which is Ethereum as the one with smart contract support. Although this can be a transparent approach, it is at its core non- viable when using on a large scale basis. The Ethereium L1 has prohibitively high levels of charges (gas costs) associated with transactions. A national election needs to process millions of transactions (votes) in a short period of time. On Ethereum, this would require millions of dollars and days to verify making the whole job worthless logically and economically insane. This fundamental drawback is what has triggered all current e-voting studies, which develop the solutions toward three different architectures: Layer-2 sidechains, alternative

high-performance L1 platforms, and hybrid or permissioned models.

II. Background and Related Works

A. Foundational Security Properties for Verifiable E-Voting

Any suggested e-voting system should in order to be a valid substitute to the existing practice, meet a strict system of security and democratic standards.

- Anonymity and Privacy: This system should provide anonymity so that no identity of a voter is ever associated with it. their cast ballot. This is the assurance of a secret vote.
- Integrity: Every cast vote that is rightfully made has to be properly registered and counted in the final tally.The invalid votes can not be added, and no valid votes may be changed or destroyed.1verifiability Two fold property.
- Individual Verifiability: A voter has to have the means to verify that his or her particular vote was.voters effectively put in the ballot box.
- Universal Verifiability: any member of the public (or any auditor) must be in a position to independently confirm that the final published total is the right amount of all validly cast.
- Fairness: The system should avoid disclosure of the partial results before the election period ends, because such information might sew confusion to the formation of future electoral choices.
- Uniqueness (Double-Voting Resistance): The principle of one person and one vote should be.

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

strictly enforced. The system should cryptographically or programmatically block any voter and ashamed on account of voting twice.

- Non-Coercibility: This is the progressive property, as compared to straightforward privacy.

B. *Architectural Approaches in Modern E-Voting Research*

Academic reaction to the shortcomings of L1 blockchains has created three main architectural fashions, both of which are illustrated in the literature used to do this paper.

- The strategy is a confession that the main net of the Ethereum is not only costly but its throughput is also low and offloads the heavy traffic of the voting transactions onto the side-chain (L2) which is capable of doing so. The most desirable model is the one proposed by Hu et al.[1] which uses the Polygon sidechain. It completely works with the Ethereum Virtual Machine (EVM) and smart contract ecosystem (e.g. Solidity, Truffle, Meta Mask) at a fraction of a cent transaction cost (or gas). It is a scalable optimization and it is a solution that talks of the issue of scalability and the costs involved hence it is a viable solution.

III. This would bypass the whole Ethereum ecosystem and instead use a more recent version of L1 blockchains that are specifically focused on high throughput. An example of this strategy is the model suggested by Chafiq et al.[3] that suggests the Solana blockchain.

IV. The Proposed HLPV System Architecture

The proposed architecture developed in this paper is the Hybrid-Layered, Privacy-Preserving Voting (HLPV) architec-ture. This system is a new synthesis, the combination of the best elements of the analyzed literature to develop an entire system which can solve the e-voting trilemma.

A. *Components or Entities System*

The basic size of system components consists of entities: programs, data (data types), and hardware. The HLPV archi-tecture comprises of four major components namely;

- Voters (V): Qualified citizens that register and vote with a wallet address of (a i) on a. smart device.1
- Election Commission (EC): This is the trusted and cen-tralized body that takes care of the system as a whole management. It has the following responsibilities: (1) its responsibilities (generating

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

the Paillier key pair) are to produce the key pair of the Paillier scheme: (pk, sk)

(2) its responsibilities (managing) It has the responsibil-ities of generating the key pair in the Paillier scheme:

(pk, sk) This is not known to implement it has the responsibilities of managing the key pair in the Paillier scheme: &(pk, sk)$ the authorized Authentication Ledger and (3) de ciphering the final encrypted tally.

- Authentication Ledger (AL): Permissioned, high-integrity blockchain, being a private blockchain, built on the hybrid cloud model. It is operated by EC and its nodes. Its sole purpose is to execute the Voter Registration smart contract and ensure a secure and timestamped and audible one database of verified addresses of voters.
- Tallying Ledger: A high throughput, low cost, decen-tralized and public L2 is referred to as Tallying Ledger blockchain. Polygon has been suggested in this paper. It is dedicated to nothing but to run the public. BallotBox smart contract Contingent on all encrypted ballots, trans-parently accepted, and execute the public homomorphic tally.

B. *The Rationale of Dual-Ledger Framework.*

- Authentication Ledger (AL): Voter registration is a high security procedure, transparency, and
- verifiable evidence, without having to be on a large scale publicly. Therefore, it is exquisitely fits the sanctioned hybrid cloud-based solution that is suggested in.[4]
- Tallying Ledger (TL): Casting and counting of ballots on the other hand, involves massively huge.specialized and high throughput, low cost, verifiable by anyone. Therefore, it is perfectly appropriate to the L2 Polygon model.
- Phase 1: Setup (EC) Before an election, the EC goes through the following set of one-time set up procedures:

1) Creates the Paillier public/ private key following aggregate operations.
2) Makes a deployment to the Authentication Ledger (AL) under deep learning.
3) Danks the BallotBox smart contract onto the Tally-ing Ledger (Polygon) which is public. This contract is launched using the election parameters:

– The list of candidates, *Circle*

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

- Starting and finishing time of voting, T start and T end.
- The Paillier public key, *pk*
- The address of the registering VoterRegistration contract on the AL to cross-check mechanism.

C. *Registration (Voter AL)*

The step develops a roster of legitimately voters with a high level of integrity and capable of auditing,providing a secure connection a link between an actual identity of the voter in the real world.

- Step 1: The voter V i registers within the period of the registration time interval (Rt start Rt end).sends their credentials (e.g., National ID) to the off-chain registration portal of the EC, which is secure.
- Step 2: The EC system anonymizes the information of the voter by developing a safe hash of his/her credentials, *hv*.
- Step 3: The EC compares the parameter hv of the EC and the official national database. Upon successful verification, this system will launch an OTP challenge to a voter registered device (e.g. phone or email).This is the working of Algorithm 1 below.
- Step 4: Voter submits the correct OTP which confirms the control of the registered device and confirmation. their wallet address a_i. number of inputs has been verified and the transaction is called by the EC on the Authentication Ledger (AL).

D. *Phase 3: Voting (Voter TL)*

This step is the second step after the secret and confidential ballot-casting exercise as outlined in.[1]

- Step 1: (Authentication): The voter contacts with his authenticated wallet address $a i.to BallotBox smart contract in the Tallying Ledger (Polygon).
- Step 2: (Ballot Creation): The voter decides to vote for a candidate $c 0 j belongs to the list of possible candidates. candidates C. The urethral interface will be a ballot result a ballot $B i = M j iM is any value larger than the number of voters $m.
- Step 3: (Encryption): The client of the voter gets the public key, pk, of the BallotBox sign and

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

encrypt their ballot: $E(B street and uses it to encrypt their ballot: $E(B underneath) = Enc(pk, M pointless).User response in the end, the voter sends a transaction to the BallotBox contract that includes their encrypted ballot $E(B_i)$.

- Step 4 (Submission): A voter transacts a transaction with the BallotBox contract with content of their encrypted ballot $E(B_i)$.

– Step 5: (Verification): This is an automatic execution of the two critical steps of BallotBox smart contract. verification checks:

– Eligibility Check: The contract makes a cross teller call to the VoterRegistration contract on the AL to ensure that the address of the sender, $a i, is available in the signed, PBFT-secured registry.

– Checking Uniqueness: This is the Checking of Such Votes: The contract is the cash price agreed upon by checked it has its own in-house mapping so to speak checked to satisfy that its internal checking is correct this speech has not already put on the ballot.

- Step 6: (Storage): The contract will take up the trans-action, should both the checks succeed. It stores the encrypted ballot on the public Tallying Ledger during the Polygon (encryption by E(B i) and values the internal.arc a i to a i = voted that will disallow duplicate voting. In case of a check refusal, the transaction is fails.

E. *Phase 4: Tallying and Reveal (EC TL)*

- Step 1 (Deadline): The deadline is at time $T end. The smart contract which is known as the BallotBox is.new programmed so as to refuse any new incoming vote transaction.
- Step 2 (Homomorphic Accumulation): The EC obtains the final encrypted sum this time $E(S) of the contract. It The secret private key of sk is used by it to decrypt this single value and obtain the plain-text result, S.
- Step 3 (Decryption): The EC obtains the final encrypted sum this time $E(S) of the contract.It The secret private key of *sk* is used by it to decrypt this single value and obtain the plain text result, S.
- Step 4 (Validation and Publication): EC publishes the result of de-encryption process of sum S. BallotBox contract. The contract authenticates $S have approved of it by comparing it with the encrypted amount. Record Finally, compute the on-chain result of using the now published sk) and store the results on-chain. verifiabil-ity. The EC may now publish sk in order to permit any

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

third party to complete ,independent required auditing of the whole election.

V. Analysis of the HLPV Model

A. *Security and Privacy Guarantees*

- Anonymity & Privacy: The dual-ledger system grants the privacy of a high level, which is multi layered. The To establish a connection between voter identity (hashed) and an anonymous wallet address, AL connects a voter real-world identity and an address of a wallet.
- Ballot Secrecy: It is one of the basic guarantees. At no point by homomorphic encryption of Paillier will it be allowed point in the process of the public tallying is any single ballot decrypted. Only the final aggregate sum is never divulged.
- Integrity: the integrity of the system is multi-dimensional. The purity of the voter list is assured on the permissioned AL, the high-finality PBFT consensus. Voting honesty of the ballot box is assured with the cryptographic uncor-ruptness of the public TL.

B. *Performance and Scalability Analysis*

- Cost-Effectiveness: The application of Polygon renders the software economically feasible to a big number. population. The evidence in gives a quantitative justifi-cation. Table 1, adapted from the results of in[1], is a comparison of the cost of major operations on Polygon and the Ethereum mainnet. (SepoliaETH testnet). The most common operation of the system is the cost of casting a vote.cheaper in order of magnitude on Polygon, making a multi-dollar purchase that much less expensive.

TABLE I

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

GAS CONSUMPTION AND COST ANALYSIS FOR TALLYING LEDGER (TL) OPERATIONS

Operation	Gas (Gwei)	Polygon Cost (ETH)	Sepolia Cost (ETH)
Deploy Contract (BallotBox)	2,863,979	0.0071598	0.008757753
User Registration (on AL)	640	0.0000064	0.00130795
Send Vote to Candidate (on TL)	410	0.0000041	0.00107873

- System Efficiency: HLPV model Authentication Ledger (AL) has the advantage of high.speed, PBFT-based archi-tecture of the hybrid-cloud design is low-latency. Table 2 projects the performance of the AL according to the empirical data used in.[4] This data shows that the registration and authentication process will be highly quick and efficient and can manage.appealing To a vast number of voters without the bottle-necks of probabilistic consensus. mechanism like PoW.

TABLE II

PROJECTED PERFORMANCE BENCHMARKS FOR AUTHENTICATION LEDGER (AL)

Performance Metric	BLFV (AL) Model (Proposed)	Baseline System	Analysis
Authentication Delay	∼1.5 ms (at 10k voters)	2.5 ms (at 10k voters)	50% reduction in delay. Suitable for real-time verification during voting phase.
Encryption Time	∼3.19 ms (at 60k voters)	7.87 ms (at 60k voters)	System maintains higher load resilience efficiently.
Latency	∼3.85 ms (at 60k voters)	7.97 ms (at 60k voters)	Low transactional latency for critical registration and validation actions.
False Rejection Rate	∼4.9% (at 10k voters)	2.9% (at 10k voters)	55% reduction in alternative attack demonstrating system security model correctness.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

TABLE III
COMPARISON OF SECURITY AND PERFORMANCE PROPERTIES

Property	Khan et al.	Dagher et al.	DVTChain[2]	HLFV (Proposed)
Anonymity	×	✓	✓	✓
Integrity	✓	✓	✓	✓
Privacy	×	✓	✓	✓
Fairness	✓	✓	✓	✓
Non-Coercibility	×	×	×	✓
Scalability	×	×	×	✓
Low Cost	×	×	×	✓

with in the real world in the context of attempting to implement it, which are also inherent to the entire e

-voting realm. The overall meta-review contained in

[5] gives an authoritative guide to the future research as it points out the least-explored areas among the academic community.

– Usability and Accessibility: HLPV architecture is technologically complicated. One of the key aspects that need to be done better in the future is the design and extensive testing of its client-side user interface. This should be simple, easy to use and completely accessible to every citizen including the disabled and those with a limited technical literacy level.

CONCLUSION

- This paper has addressed the challenging issues of se-curity, scalability, and privacy that have prevented the e-voting process to become more mainstream. Examining the vulnerabilities of the old school and centralized structures 1 and analyzing the choke points of the first-gen blockchain performances, we identified the primary areas of weakness that we should address. We proposed a new Privacy-Preserving Voting (HLPV) architecture with Hybrid-Layered architecture. The point is to sew the most interesting fragments of the research world to create an

Encryption Time voting phase. ~3.19 ms (at 60k voters) 7.87 ms (at 60k voters) System maintains higher load re-silience efficiently. actual, functional system.

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

Latency ~3.85 ms (at 60k voters) 7.97 ms (at 60k voters) Low transactional latency for crit-ical registration and validation ac-tions. False Rejection Rate~4.9% (at 10k voters) 2.9% (at 10k voters) 55% reduction in alternative at- tack demonstrating system security model correctness.

VI. DISCUSSION

- Comparative Evaluation :The HLPV system architecture takes the best of a collection of models and constructs an architecture that is stronger than its components. With a few modifications to the comparative analyses in [1] and [2] we can demonstrate the position of the HLPV in the contemporary academic environment. Table 3 identifies HLPV as hitting the nail on the head over all the crucial features that previous models have failed to capture particularly the elusive balance between non-coercibility, scalability and cost-effectiveness.
- Future Research Limitations and Prospects:

– Although the HLPV model is a sound technical solution, there are issues that would have to be dealt HLPV framework performs three functions: A permissioned authentication ledger (AL) with the finest integrity ensures the safety of voter sign-up and is correctly timed, absolutely. For example, a super-scalable and inexpensive Tallying Ledger (TL) which resides in the Polygon sidechain, such that individuals can place a cast even when they are out of range. The Paillier homomorphic encryption scheme that moves to lock the secrecy of the ballots and allow all people to check the final number. That two-ledger system clears the e-voting trilemma. We have analyzed it, and supported by the performance data and the cost figures provided in the source papers 1[1],[4], the HLPV design is found to be fast, cheap, and safe. Even better, it is among the few models that does ensure non-coercibility, something that is easily forgotten. On the whole, HLPV blueprint is a giant leap in the direction of scalable, safe, and really democratic electronic voting systems.

6 REFERENCE

Primary Source

1) Hu, Y. Peng, S. (2024), Decentralized Blockchain based voting system. Procedia Computer Science, 247, 1304-1313.
2) Alvi, S. T., Uddin, M. N., Islam, L., and Ahamed,

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

S. (2022). DVTChain: A blockchain-based to provide the security of the digital voting system, there should be a decentralized mechanism. Journal of King Saud University - Computer and Information Sciences, 34(9): 6855-6871.

3) Chafiq, T., Azmi, R., Mohammed, O. (2024). Electronic voting systems based on blockchain technology: A case study in Morocco. International Journal of Intelligent Networks 5, 38-48.
4) Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., and Jawahar, M. (2024). Cloud-based hybrid blockchain technology e-voting system. Journal of Safety Science and Resilience, 5, 102-109.
5) Berenjestanaki, M. H., Barzegar, H. R., El Ioini, N., and Pahl, C. (2024). Blockchain-Based E Voting Systems: Technological Review. Electronics, 13(17).

Secondary Sources

1) Gibson, J. P., Krimmer, R., Teague, V., and Pomares, J., (2016) A review of e-voting: the past, present and future." Annals of Telecommunications, 71, 279-286.
2) Cabuk, U. C., Adiguzel, E., and Karaarslan, E. (2020) "A survey on feasibility and suitability. of blockchain methodology to the e-voting systems. arXiv preprint arXiv:2002.07175.
3) Chaum, D. L. (1981) Untraceable electronic mail, return addresses and digital pseudonyms. Communications of the ACM, 24(2), 84-90.
4) Ewing, P. (2019) "What you need to know about the US election security and voting machines. NPR. Blockchain Association, 1(2).
5) Curran, K. (2018) "E-voting on the blockchain." The Journal of the British
6) Kadam, S., Chavan, K., Kulkarni, I., and Patil, A. (2019) "Survey on digital e-voting system. with blockchain technology. International Journal of Advance Scientific Research and Engineering Trends.
7) Wang S., Han W., and Chen K. (2006) "Problems and advances in e-voting research. Computer Engineering, 32(15): 4.
8) Zheng X. (2017) "The alienation and moral contem-plation of the WeChat public voting: A compared to traditional public voting."

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor:10.2
Subject: Computer Science and Engineering

Author's Declaration

As an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my hole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible, shuffled, or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who find trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher, then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website, or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Pushkar Pandey
Karan Bisht
Dr. Maneesh Upadhya

****