

Article

A Blockchain-Based Bimodal Voter Accreditation System (Block-BVAS): A Framework for Adoption in Electronic Voting Systems

Henry Ohiani Ohize ^{1,2,*} , Adeiza James Onumanyi ³ , Lukman Adewale Ajao ⁴ , Buhari Ugbede Umar ⁵ , Abdulrahman Surajudeen ², Joseph Mona Ijalija ², Samuel Ayomide Olosunde ², Abdulhakeem Omeiza Abdullahi ² and Olayemi Mikail Olaniyi ⁶ 

- ¹ Department of Electrical and Electronics Engineering, Confluence University of Science and Technology, Osara 264103, Kogi State, Nigeria
 - ² Department of Electrical and Electronics Engineering, Federal University of Technology Minna Gidan Kwano, Minna 920102, Niger State, Nigeria; abdulrahman.m1801330@st.futminna.edu.ng (A.S.); josephijalija@gmail.com (J.M.I.); samolosunde@gmail.com (S.A.O.); abdulhakeemomeiza2016@gmail.com (A.O.A.)
 - ³ Next Generation Enterprises and Institutions, Council for Scientific and Industrial Research (CSIR), Pretoria 0001, South Africa; aonumanyi@csir.co.za
 - ⁴ Department of Mechatronics Engineering, Federal University of Technology Minna Gidan Kwano, Minna 920102, Niger State, Nigeria; ajao.wale@futminna.edu.ng
 - ⁵ Department of Computer Engineering, Federal University of Technology Minna Gidan Kwano, Minna 920102, Niger State, Nigeria; buhariumar@futminna.edu.ng
 - ⁶ Department of Computer Science, National Open University of Nigeria, Abuja 900108, Nigeria; omolaniyi@noun.edu.ng
- * Correspondence: henryohize@futminna.edu.ng or ohizeho@custech.edu.ng

Abstract

Despite significant advances in electronic voting technologies, voter accreditation in many electoral systems remains vulnerable to identity fraud, database tampering, equipment failure, and centralized security breaches. Existing accreditation solutions often rely on single-modal biometric authentication and centralized architectures, limiting their robustness, transparency, and public trust. This paper proposes a Blockchain-based Bimodal Voter Accreditation System (Block-BVAS), together with a practical framework for its deployment in electronic voting systems. The proposed system integrates multimodal biometric authentication using facial and fingerprint recognition with a private Ethereum blockchain and conventional cryptographic mechanisms to provide secure, tamper-resistant, and auditable voter accreditation to provide secure, decentralized, and tamper-resistant voter accreditation. A Raspberry Pi 5 serves as the embedded processing platform, demonstrating the feasibility of implementing the framework on cost-effective hardware. By combining distributed-ledger technology with encrypted biometric verification, the proposed architecture enhances the integrity, confidentiality, and immutability of election-related records while addressing limitations associated with single-factor authentication and conventional centralized record management. Experimental evaluation of the biometric authentication module performed effectively, with fingerprint recognition achieving an average authentication accuracy (AA) of 97.8% and facial recognition averaging 95.1%. The blockchain storage overhead (BSO) displayed a near-linear growth pattern relative to the number of transactions, consistent with theoretical expectations for blockchain architectures. Reliability analysis indicated system uptime exceeding 95%, with only minimal operational failures recorded during the test period. This blockchain implementation further demonstrated reliable transaction processing and secure record management, indicating the effectiveness



Academic Editor: Maurizio Talamo

Received: 27 April 2026

Revised: 20 August 2026

Accepted: 21 August 2026

Published: 27 August 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

of the proposed Block-BVAS in enhancing the security, transparency, and trustworthiness of electronic voter accreditation.

Keywords: blockchain; electronic voting; block-BVAS; election; biometrics; fingerprint; raspberry Pi5

1. Introduction

Electronic voting (e-voting) provides a modern alternative to conventional paper-based systems by leveraging digital technologies to facilitate the casting and counting of votes [1]. With the growing adoption of digital infrastructure worldwide, e-voting offers significant potential to enhance the efficiency, accessibility, and accuracy of electoral processes [2]. Existing e-voting technologies range from internet-based platforms accessible via personal devices to specialized machines deployed at polling stations, reflecting the diversity and continual evolution of voting innovations [3].

Despite these advantages, e-voting systems face challenges related to cybersecurity, data privacy, accessibility, and the digital divide. Addressing these issues is essential to ensuring system reliability, voter confidence, and electoral integrity. Furthermore, the diversity of e-voting systems necessitates comparative assessment to determine their compliance with fundamental criteria such as security, transparency, usability, and cost-effectiveness. To this effect, a comparative overview of different traditional e-voting systems highlights their relative advantages and limitations. For example, direct recording electronic (DRE) voting machines, as described in [4], offer the benefit of instant vote recording and tallying with improved accessibility for persons with disabilities; however, they are often criticized for their vulnerability to glitches, cyberattacks, and the lack of a verifiable audit trail without printed records. On the other hand, optical scan systems proposed in [5] provide verifiable paper ballots and a familiar interface for voters, yet they remain susceptible to scanning errors and depend heavily on the quality of the scanners used. Internet Voting, discussed in [6], enhances accessibility for remote voters and reduces reliance on physical infrastructure but introduces heightened cybersecurity risks and may widen the digital divide among users. Lastly, hybrid systems, as presented in [7], merge the strengths of efficiency and auditability to bolster voter confidence, though they are often expensive, technically complex, and prone to mechanical failures during operation.

Blockchain technology has emerged as a promising solution to address a number of the above challenges. In particular, the decentralized, immutable, and transparent architecture of blockchain enables secure and verifiable storage of voting records [8]. Essentially, the integration of blockchain into e-voting systems can mitigate issues of data manipulation and unauthorized access, thus enhancing the credibility and auditability of elections.

Consequently, in the present study, a blockchain-based e-voting framework is proposed and implemented, which incorporates fingerprint and facial recognition for robust voter authentication. The proposed design enhances system security, reliability, and user experience, offering a transparent and user-friendly solution that promotes voter trust and participation. The major contributions of this work are as follows:

1. Implementation of Block-BVAS prototype on a private Ethereum blockchain configured with a DPoS consensus mechanism.
2. Deployment of multimodal biometric authentication using Raspberry Pi 5 for identity verification.
3. A layered system architecture to improve scalability and performance.

4. Development of a Java EE-based e-voting web application using the NetBeans IDE, deployed on a native GlassFish server and integrated with a MySQL database and blockchain backend.
5. Prototyping of the proposed blockchain-based voter accreditation system (Block-BVAS) that combines blockchain and biometric validation.

The remainder of this paper is organized as follows. Section 2 reviews related works. Section 3 presents an overview of the block-BVAS. Section 4 details the system level model of the Block-BVAS and Section 5 presents the design and implementation methodology. Section 6 presents the performance evaluation metrics, while Section 7 discusses the experimental results obtained. Section 8 discusses the technical challenges and future directions for the implemented Block-BVAS. Finally, Section 9 concludes the paper.

2. Related Work

A substantial body of the literature exists on the design and implementation of electronic voting (e-voting) systems. Despite this progress, many of these systems continue to face fundamental challenges such as inadequate security, poor scalability, and limited voter trust, which raise concerns about the integrity and transparency of electoral outcomes [9,10]. Recent efforts have turned toward integrating blockchain technology and biometric authentication to strengthen data security and ensure verifiable voter accreditation. This section critically reviews these developments and identifies the key gaps that the proposed blockchain-based bimodal voters accreditation system (Block-BVAS) aims to address. An overview of selected blockchain-based e-voting system implementations is presented in Table 1 for readers interested in comparative studies of related approaches.

Table 1 summarizes major contributions in blockchain-enabled biometric e-voting, covering frameworks that combine distributed ledger technology, cryptographic hashing, and biometric identity verification to enhance transparency and voter confidence. These works demonstrate the promise of blockchain for secure digital elections and include hybrid models that integrate Internet of Things (IoT) devices, secure multiparty computation, and smart contracts. However, despite their technical merits, several unresolved issues continue to limit the practical deployment of such systems in large-scale elections.

From an engineering standpoint, most existing studies provide conceptual frameworks without fully functional prototypes that validate real-time performance or system scalability under field conditions. For instance, the works of [4,11] leveraged blockchain's immutability and transparency to safeguard election integrity, using biometric verification and cryptographic hashing for voter authentication. Similarly, projects such as d-BAME [12] and Votereum [13] explored Ethereum-based models that combine blockchain with secure multiparty computation, IoT connectivity, and smart contract logic to improve trust and scalability. In addition, studies like [7,14] investigated biometric data integration to prevent double voting and voter impersonation, utilizing physiological features for secure identification.

While these contributions represent important milestones, the literature still reveals gaps that hinder the full realization of blockchain-biometric e-voting systems. Thus, Table 2 provides a comparative summary highlighting these gaps relative to our proposed work. First, to the best of the authors' knowledge, there are few reported works that demonstrate a complete operational prototype integrating multimodal biometrics with blockchain on a lightweight embedded platform such as Raspberry Pi 5. Second, privacy-preserving mechanisms, including zero-knowledge proofs and smart contract-driven data integrity, remain underexplored in the reviewed systems. Third, many designs lack layered architectures to support modular scalability and high system performance. Finally, usability

and transparency, which is essential for public acceptance are often treated as secondary considerations rather than integral design objectives.

In summary, the reviewed literature indicates that while blockchain and biometrics offer complementary strengths (i.e., immutability and secure identity verification), their integration remains largely theoretical or limited to partial simulations. This study addresses this gap by providing a fully implemented framework that integrates blockchain with multimodal biometric verification, conventional cryptographic mechanisms, and a layered architectural design intended to support scalable deployment. The proposed Block-BVAS prototype thus represents a significant step toward practical, transparent, and tamper-resistant e-voting solutions suitable for real-world election environments.

Table 1. Review of Existing Work on Combining Blockchain with Biometric Authentication.

Ref.	Year	Main Focus	Specific Contributions
[15]	2026	IoT biometric evoting	End-to-end IoT-biometric-enabled secure blockchain-based e-voting system. Integration of ESP32, AFIS, InsightFace and Ethereum technology
[16]	2025	Ethereum Layer 2 Solutions and Machine Learning	Rollups and ML optimisation. Ethereum Layer 2 frameworks, emphasizing their integration with machine-learning techniques.
[17]	2025	Blockchain-powered e-voting for transparency and security.	Integration of blockchain and biometric verification utilising Raspberry Pi 4, integrated with multimodal biometric (facial and fingerprint) authentication systems, programmed with DLIP algorithm to optimize image detection and recognition.
[11]	2023	Blockchain-powered e-voting for transparency and security.	Bridging research gaps in in-person e-voting; integration of blockchain and biometric verification using Hyperledger Fabric; user interface tailored for electoral stakeholders.
[4]	2022	Blockchain-based digital voting system.	Smart contracts for secure automation; voter anonymity via hashed data; mobile number verification and OTP for secure authentication.
[7]	2022	Integration of blockchain and biometrics for e-voting.	“BieVote” framework to improve voting integrity; securing biometric data for scalability and real-world application.
[12]	2021	Remote e-voting with secure multiparty computation.	d-BAME model for large-scale mobile voting; prevention of double voting, anonymity, and coercion.
[18]	2021	Blockchain-IoT e-voting system.	Hierarchical blockchain for scalability; biometrics-based secret keys; system analysis using Ethereum and MATLAB.
[19]	2020	Secure smart card for blockchain e-voting.	Arduino-based key management with RFID and NodeMCU; Paillier algorithm for secure storage.
[14]	2020	Blockchain for African electoral systems.	Biometric registration and verification; blockchain-logged voting results; accessibility across network nodes.
[20]	2020	Blockchain and machine learning for e-voting.	Merkle trees, smart contracts, intrusion detection placement in hybrid blockchain systems.
[21]	2019	Blockchain-based voting system.	Ethereum for data integrity and anonymity; two-step voter authentication; Merkle Trees for reliable voting records.
[22]	2019	Decentralized e-voting with blockchain and smart contracts.	Cryptographic methods for secure, transparent voting; encryption to overcome traditional limitations.
[23,24]	2019	Decentralized blockchain e-voting.	Ethereum smart contracts using Truffle framework; optimized architecture for scalability.
[13]	2019	Ethereum-based e-voting system.	“Voteum” on Rinkeby test network; analysis of architecture and functionality.
[6]	2019	Secure e-voting using blockchain.	Smart contracts, zero-knowledge proofs, Proof-of-Authority consensus; electronic ID authentication.

Table 2. Gaps in the Literature.

Ref	Year	BB	HM	WA	eV	MA	MB	HB	PB	PK	SK	D	RP	AD
[25]	2007	X	X	✓	✓	X	X	X	X	X	X	X	X	X
[9]	2013	X	X	✓	✓	X	X	X	X	X	X	X	X	X
[26]	2013	X	X	✓	✓	X	X	X	X	X	X	X	X	X
[27]	2015	X	X	✓	✓	X	✓	X	X	X	X	X	X	X
[28]	2016	✓	✓	X	✓	X	X	X	X	✓	✓	✓	X	X
[29]	2017	✓	✓	✓	✓	X	X	X	X	X	✓	✓	X	X
[30]	2018	✓	✓	✓	✓	✓	X	✓	X	✓	✓	✓	X	X
[31]	2018	✓	✓	✓	✓	X	X	X	✓	✓	✓	✓	X	X
[6]	2018	✓	✓	X	✓	X	X	X	X	✓	✓	✓	X	X
[32]	2018	✓	✓	X	✓	X	✓	✓	X	X	✓	✓	X	X
[33]	2018	✓	✓	X	✓	X	✓	X	X	X	X	✓	X	✓
[34]	2018	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓	X	X
[35]	2019	✓	✓	✓	✓	X	X	X	✓	✓	✓	✓	X	X
[36]	2019	✓	X	✓	✓	X	X	✓	✓	✓	✓	X	X	X
[37]	2019	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	X	X
[38]	2020	✓	✓	✓	✓	X	X	X	✓	✓	✓	✓	X	✓
[39]	2020	✓	✓	✓	✓	X	X	✓	X	✓	✓	✓	X	✓
[40]	2020	✓	✓	✓	✓	X	X	✓	✓	✓	✓	X	X	✓
[41]	2020	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	X	✓
[42]	2020	✓	X	✓	✓	X	X	✓	✓	✓	✓	✓	X	X
[43]	2020	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	X	✓
[44]	2021	✓	✓	X	✓	X	X	X	✓	✓	✓	✓	X	X
[45]	2021	X	X	X	✓	X	X	X	X	✓	✓	X	X	✓
[46]	2022	✓	✓	X	✓	X	X	✓	X	✓	✓	✓	X	X
[47]	2022	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	X	X
[46]	2022	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	X	✓
[48]	2022	✓	✓	X	✓	X	✓	✓	✓	✓	✓	✓	X	✓
[15]	2026	✓	✓	✓	X	X	X	X	✓	X	X	✓	X	✓
PS	2026	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Legend: BB = blockchain-based, HM = hashing Mechanism, WA = website application-based; MA = multimodal authentication, eV = electronic voting, MB = microcontroller-based system developed. HB = Hyperledger Blockchain, PB = public blockchain, PK = primary key, SK = secondary key, D = decentralization, RP = Raspberry Pi 5, AD = architecture described; ✓ = the feature is present or addressed; X = the feature is absent or not addressed; PS = proposed system.

3. Overview of Block-BVAS

This section briefly discusses the key principles of blockchain technology, followed by its integration with biometric verification and the unique implementation features that characterize Block-BVAS. Understanding these underlying principles is essential for appreciating how the system leverages blockchain's decentralized properties to enhance the integrity and transparency of e-voting. Firstly, blockchain technology, founded on distributed ledger principles, ensures immutability, transparency, and traceability of data, thereby reducing the risks of manipulation and human error [17,49]. When applied to e-voting, blockchain can provide a distributed and tamper-resistant mechanism for voter

accreditation, vote recording, and result management. In the implemented prototype, the private Ethereum network distributes election transactions among authorized validator nodes, while biometric templates remain in secure local off-chain storage. The distributed blockchain ledger reduces the risk of unauthorized modification of election transactions and provides a verifiable audit trail; however, the current centralized storage of biometric templates remains a potential single point of failure.

Building upon these fundamental properties, a blockchain network maintains a continuously growing ledger of transactions replicated across multiple nodes [41,50]. Its cryptographic foundations, including public-key encryption, hashing, digital signatures, and consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA) collectively guarantee data integrity, authenticity, and non-repudiation [51,52]. These mechanisms establish the technical backbone of trust that makes blockchain suitable for mission-critical applications such as national elections. For institutional use, private blockchain frameworks like Hyperledger Fabric offer controlled access, fine-grained permissioning, and enhanced privacy, making them ideal for regulated environments such as national electoral commissions [53]. Consequently, the proposed Block-BVAS architecture adopts this private blockchain model, as illustrated in Figure 1.

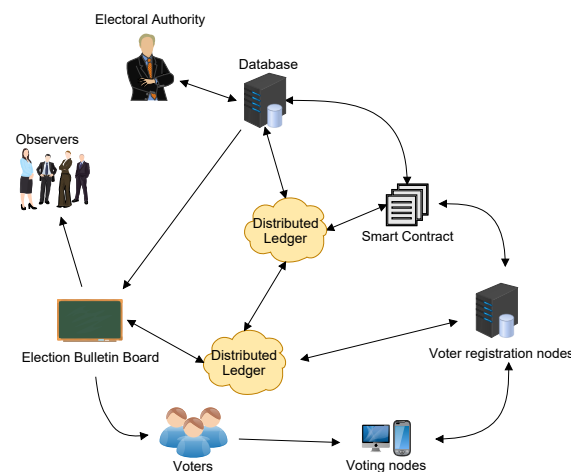


Figure 1. Private Blockchain Architecture for Block-BVAS [49].

While blockchain ensures the security and transparency of transactional data, it does not inherently verify the authenticity of individual voters. To address this, biometric authentication is employed to safeguard voter identity by leveraging unique biometric characteristics, such as fingerprint patterns and facial characteristics, for secure identification [54]. Previous works [55,56] confirmed that fusing cryptographic mechanisms with biometric recognition enhances authentication robustness; however, many existing systems still suffer from limited transparency, centralized storage vulnerabilities, and a lack of real-time verifiability, emphasizing the need for a more integrated approach.

Responding to these limitations, Block-BVAS combines blockchain's decentralized security with bimodal biometric authentication implemented on a Raspberry Pi 5 platform. The system captures and verifies voters using both facial and fingerprint modalities, encrypts biometric templates for secure local storage, and records verified election transactions on the blockchain. This integration supports transaction synchronization, tamper-evident audit trails, and reliable biometric verification performance within the evaluated prototype environment. By merging blockchain's immutability with the precision of biometric verification, Block-BVAS provides a secure, transparent, and trustworthy foundation for modern electronic voting infrastructure, particularly applicable to emerging democracies in Africa seeking reliable and auditable digital election systems.

4. System Model and Block-BVAS Framework

This section presents the Block-BVAS architecture, as illustrated in Figure 2. Implementation of the Block-BVAS system was achieved using a Raspberry Pi 5 microcontroller, a fingerprint and facial recognition sensor, an LCD, a keypad, and a WiFi module to connect to a cloud-based blockchain network and database server. Each component of the architecture is discussed as follows:

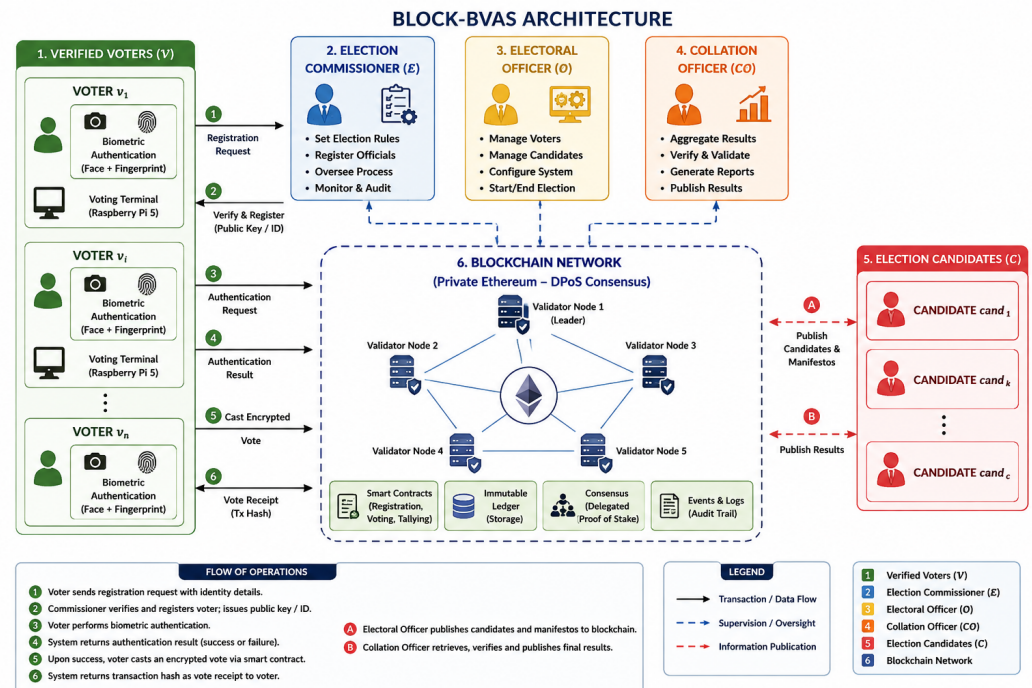


Figure 2. Block-BVAS System Architecture.

4.1. System Model

The Block-BVAS model consists of six entities, each playing distinct roles within the system. These entities are defined as follows:

1. **Verified Voters:** Denoted by the set $\mathbb{V}$, representing all eligible voters. Each voter is defined as $v_i \in \mathbb{V}$, where $1 \leq i \leq n$ and n is the total number of eligible voters.
2. **Election Commissioner:** Represented as $\mathbb{E}$, responsible for overseeing the election process and ensuring compliance with election rules.
3. **Electoral Officer:** Denoted as $\mathbb{O}$, tasked with managing operational aspects of the election.
4. **Collation Officer:** Represented as $\mathbb{CO}$ and responsible for aggregating and verifying the election results.
5. **Election Candidates:** Represented by the set $\mathbb{C}$, containing all eligible candidates running in the election. Each candidate is defined as $cand_k \in \mathbb{C}$, where $1 \leq k \leq c$ and c is the total number of candidates.
6. **Blockchain Network:** The decentralized system used to securely store and verify election-related data, ensuring transparency and integrity.

Each entity has a specific and non-overlapping role, which contributes to the overall functionality and security of the voting scheme.

4.2. Block-BVAS Framework

The framework for the use and deployment of Block-BVAS is discussed as follows.

4.2.1. Vote Set-Up

The vote set-up phase establishes the cryptographic foundations required for secure communication, authentication, and verification during the election process. In this stage, the election commissioner and the electoral officer each generate a private key, denoted by x_e and x_o , respectively, where $x_e, x_o \in \mathbb{Z}_p$. These private keys are large random integers selected from the finite field $\mathbb{Z}_p$, ensuring that they remain confidential and known only to their respective owners.

To derive the corresponding public keys, the Block-BVAS algorithm performs modular exponentiation using a pre-defined generator g of a cyclic group under modulo- p arithmetic. The public keys are computed as:

$$y_e = g^{x_e} \pmod{p}, \quad (1)$$

$$y_o = g^{x_o} \pmod{p}, \quad (2)$$

where y_e and y_o represent the election commissioner's and electoral officer's public keys, respectively.

Here, the generator g serves as the base element of the multiplicative group $\mathbb{Z}_p$, chosen such that its successive powers modulo p can produce every nonzero element in the group. This property guarantees that each unique private key corresponds to a distinct public key, thereby ensuring strong one-way mapping, which is a fundamental requirement for secure cryptographic operations such as digital signatures, authentication, and encryption within the Block-BVAS framework.

Through this setup, both officials establish secure key pairs that serves as a foundation for all subsequent phases of the e-voting process. This stage enables verifiable and tamper-resistant interactions between the election authority, blockchain nodes, and registered voters.

4.2.2. Voter Registration

The voter registration phase establishes the foundation for secure participation in the e-voting process. In this phase, each voter's identity and eligibility are verified before being added to the blockchain-based electoral roll. Voters are required to provide valid identification documents and undergo multimodal biometric accreditation (facial and fingerprint recognition) to prevent impersonation or duplicate registration. Once eligibility is confirmed, cryptographic credentials are generated to ensure that every voter can be uniquely identified and securely authenticated throughout the election lifecycle. The process proceeds as follows:

1. Voter key generation and registration: Each eligible voter v_i generates a private key $x_i \in \mathbb{Z}_p$, which is a large random integer kept secret by the voter. Using this private key, Block-BVAS computes the corresponding public key as:

$$y_i = g^{x_i} \pmod{p}. \quad (3)$$

Again, g denotes a generator of the cyclic group $\mathbb{Z}_p$, ensuring that each voter's key pair (x_i, y_i) is unique and computationally infeasible to reverse. The voter's public key y_i is then securely submitted to the election officials during registration for validation and certification. This step ensures that all registered voters possess unique cryptographic identities, which enables the system to later verify voter credentials without directly exposing the underlying cryptographic private key, thereby supporting authentication and credential integrity.

2. Signing the voter's public key: To guarantee the integrity and legitimacy of voter identities, the election commissioner validates and digitally signs each voter's public key. The signature process authenticates that the key belongs to a verified individual and prevents the registration of fraudulent credentials. The signing procedure is as follows:

- (a) Random number selection: A random number u_i is chosen such that it is coprime with $p - 1$; that is, $1 \leq u_i \leq p - 1$ and $\gcd(u_i, p - 1) = 1$, where $\gcd$ represents the greatest common divisor of the two integers $u_i, p - 1$. This ensures that u_i has a modular inverse u_i^{-1} modulo $p - 1$, which is a requirement for computing the signature.
- (b) Computation of signature values: The following quantities are then derived by Block-BVAS:

$$w_i = g^{u_i} \pmod{p}, \quad (4)$$

$$s_i = [h(y_i) - x_o w_i] u_i^{-1} \pmod{p}, \quad (5)$$

where $h(y_i)$ is the hash of the voter's public key, and x_o denotes the private key of the electoral officer. The hash function ensures that even small changes in y_i result in entirely different outputs, reinforcing data integrity.

- (c) Signature formation: The pair (w_i, s_i) constitutes the digital signature associated with the voter's public key.
- (d) Recording the certified key: The final signed record is expressed as:

$$y_i \parallel (w_i, s_i), \quad (6)$$

where " $\parallel$ " represents concatenation. This signed tuple is stored on the blockchain as part of the voter's registration data, which ensures a verifiable and tamper-resistant registration record.

Through this process, Block-BVAS ensures that every registered voter is both biometrically authenticated and cryptographically certified. The combination of biometric verification, hashing, and digital signatures prevents identity forgery, eliminates duplicate entries, and enables transparent verification of voter authenticity without compromising privacy. This dual-layered registration mechanism forms the cornerstone of the system's trust model and provides the foundation for the subsequent phases of secure voting and result validation.

4.2.3. Acquiring Ballot

The ballot acquisition phase marks the beginning of the voting process, where each eligible voter securely obtains a unique digital ballot for casting their vote. This phase integrates blockchain technology to guarantee transparency, traceability, and integrity in ballot generation, assignment, and distribution. Each transaction within this process is recorded on the blockchain, ensuring a verifiable and tamper-evident trail. The procedure for acquiring a ballot in the Block-BVAS system is outlined as follows:

1. Ballot generation: The election commissioner generates a set of encrypted ballots, denoted as $\mathbb{B} = \{b_1, b_2, \dots, b_m\}$. Each ballot $b_j \in \mathbb{B}$ is uniquely identified and associated with a specific election event. Using the commissioner's public key y_e , every ballot is encrypted to ensure confidentiality:

$$b_j = E(y_e, \text{Ballot_ID}_j), \quad (7)$$

where E is the encryption function and Ballot_ID_j represents the unique identifier of the j -th ballot. To maintain transparency, a hashed record of all generated ballots is published on the blockchain as:

$$\text{Hash}(\mathbb{B}) = \text{SHA256}(\{b_1, b_2, \dots, b_m\}), \quad (8)$$

making any unauthorized alteration to the ballots immediately detectable. This mechanism ensures that all ballots are verifiable, non-repudiable, and resistant to duplication or tampering.

2. Voter permutation: To reduce direct association between voter registration records and ballot identifiers, the electoral officer applies a random permutation π to the ballot set. The permuted ballots are expressed as $B_\pi = \pi(B)$, and the corresponding mapping is maintained by the election system for ballot assignment and verification. This procedure is intended to reduce direct linkage between voter registration information and assigned ballot identifiers; however, formal end-to-end voter–ballot unlinkability is beyond the scope of the present prototype.
3. Requesting a ballot: Each verified voter v_i submits a ballot request to the electoral officer, including their previously signed public key $y_i \parallel (w_i, s_i)$. This request is permanently logged on the blockchain to guarantee auditability and traceability:

$$\text{Request}_{v_i} = \text{Blockchain_Log}(y_i \parallel (w_i, s_i)). \quad (9)$$

The blockchain log serves as an immutable record confirming that the voter has legitimately requested a ballot and preventing duplicate requests.

4. Ballot assignment and encryption: Once the voter's signature is verified, the electoral officer assigns a random ballot $b_j \in \mathbb{B}_\pi$ to the voter. To ensure confidentiality, the ballot is encrypted using the voter's public key y_i :

$$b'_j = E(y_i, b_j), \quad (10)$$

and the assignment is then recorded on the blockchain as:

$$\text{Assignment}_{v_i} = \text{Hash}(b'_j). \quad (11)$$

This double encryption mechanism, first by the commissioner and then by the voter's public key, ensures that ballots remain confidential and uniquely bound to their recipients.

5. Voter decrypts the assigned ballot: Upon receiving the encrypted ballot b'_j , the voter uses their private key x_i to perform decryption:

$$b_j = D(x_i, b'_j), \quad (12)$$

where D denotes the decryption function. Only the rightful voter possessing x_i can retrieve the valid ballot content, hence guaranteeing ballot ownership and integrity.

Through this process, Block-BVAS provides each eligible voter with a unique and verifiable ballot. The combination of blockchain-based record keeping, cryptographic encryption, and randomized ballot assignment is intended to strengthen ballot confidentiality, traceability, and resistance to duplicate requests and unauthorized modification.

4.2.4. Voting for a Candidate

The voting phase represents the core of the Block-BVAS process, during which each voter securely casts their choice while maintaining confidentiality and data integrity. The use of blockchain technology provides an immutable and auditable record of submitted vote transactions, while cryptographic mechanisms are used to protect the confidentiality of the recorded vote information:

1. Ballot preparation: The voter encodes their chosen candidate $cand_k \in \mathbb{C}$ onto their assigned ballot b_j . The encoded ballot is represented as:

$$b_j^* = \text{Encode}(cand_k, b_j), \quad (13)$$

where the function $\text{Encode}(\cdot)$ embeds the selected candidate information within the digital ballot structure. This encoding ensures that the vote content is bound to a valid ballot and can later be verified on the blockchain without exposing the voter's preference.

2. Vote encryption: The voter encrypts the prepared ballot using the election commissioner's public key y_e :

$$v_j = E(y_e, b_j^*), \quad (14)$$

where E denotes the encryption function. This operation guarantees that the vote remains confidential and cannot be altered or read by unauthorized parties during transmission or storage on the blockchain.

3. Vote submission: The encrypted vote v_j is then transmitted to the blockchain network for recording and verification:

$$\text{Vote_Log} = \text{Blockchain_Log}(v_j). \quad (15)$$

Once logged, the blockchain permanently stores the encrypted vote in a distributed ledger, providing an immutable record that ensures transparency and auditability. The decentralized nature of this process prevents any single authority from modifying or deleting votes, thereby upholding the integrity of the election.

Through this mechanism, Block-BVAS enables a secure and transparent voting experience where every ballot is confidentially encoded, encrypted, and verifiably recorded on the blockchain, ensuring fairness, privacy, and trust throughout the election process.

4.2.5. Vote Tallying

The vote tallying phase represents the final stage of the Block-BVAS process, where all submitted votes are aggregated, decrypted, and verified to determine the election outcome. Blockchain technology ensures that the tallying process remains transparent, tamper-resistant, and publicly auditable. The sequence of operations in this phase is described as follows:

1. Vote collection: All encrypted votes v_j are retrieved from the blockchain ledger, which serves as the authoritative and immutable source of recorded votes. The complete set of votes is represented as:

$$\mathbb{V}_s = \{v_1, v_2, \dots, v_n\}. \quad (16)$$

This ensures that only legitimate votes previously logged on the blockchain are included in the counting process.

2. Vote decryption: The election commissioner decrypts each vote using their private key x_e to reveal the encoded ballot content:

$$b_j^* = D(x_e, v_j), \quad (17)$$

where $D(\cdot)$ denotes the decryption function. The decryption process restores each encrypted vote to its encoded form. The system maintains voter registration information separately from the recorded vote data to reduce direct association between voter credentials and ballot selections.

3. Candidate aggregation: The decoded ballots b_j^* are grouped and tallied according to the selected candidates $cand_k \in \mathbb{C}$. The total votes $T(cand_k)$ for each candidate are computed as:

$$T(cand_k) = \sum_{j=1}^n \delta(b_j^*, cand_k), \quad (18)$$

where $\delta(b_j^*, cand_k)$ is an indicator function defined as:

$$\delta(b_j^*, cand_k) = \begin{cases} 1 & \text{if } b_j^* \text{ corresponds to a vote for } cand_k, \\ 0 & \text{otherwise.} \end{cases} \quad (19)$$

This formulation ensures that each valid vote contributes exactly one count to the appropriate candidate, which prevents double counting or unauthorized additions.

4. Result verification and announcement: The final tally results are hashed and published on the blockchain to guarantee transparency and prevent post-tally manipulation:

$$\text{Result_Log} = \text{Hash}(T(cand_1), T(cand_2), \dots, T(cand_c)). \quad (20)$$

The candidate with the highest tally value is determined as:

$$\text{Winner} = \arg \max_{cand_k \in \mathbb{C}} T(cand_k). \quad (21)$$

By recording the results on the blockchain, every stakeholder can independently verify the outcome, which ensures public confidence in the election process.

Through this sequence, Block-BVAS guarantees that vote counting is verifiable, transparent, and immutable. The use of blockchain for result publication reinforces trust and accountability, hence ensuring that the declared outcome faithfully reflects the collective will of the voters.

5. Block-BVAS Software and Hardware Implementation

This section describes the practical deployment of the proposed e-voting scheme using Raspberry Pi 5 as the main processing unit, together with a keyboard for manual input and multimodal sensors for secure voter authentication. The implementation combines the computational capability of Raspberry Pi 5, the reliability of biometric sensors, and the transparency of blockchain technology to achieve a secure, efficient, and user-friendly voting system. The overall setup integrates both hardware and software components that operate together to ensure data confidentiality, transparency, and seamless interaction during the voting process.

5.1. Hardware Implementation

The hardware components required for the implementation are described as follows:

1. **Raspberry Pi 5:** This serves as the central processing unit of the system. It performs key generation, encryption, blockchain communication, and biometric data processing. Its high processing power and low energy consumption makes it suitable for real-time operations in field deployments.
2. **Keyboard:** It provides manual input for users during registration, system configuration, and ballot acquisition phases, thus ensuring accessibility where biometric sensors cannot be used.
3. **Multimodal sensors:** These include a fingerprint scanner and a facial recognition camera, which work together to ensure accurate and reliable voter authentication by validating unique physiological traits.
4. **Touchscreen display:** This provides an interactive graphical user interface that allows voters to navigate registration, ballot selection, and voting processes easily.
5. **Secure digital (SD) card:** It stores the operating system, the application software, and the blockchain ledger, which ensures secure and persistent data storage.
6. **Power supply unit:** This delivers stable electrical power to the Raspberry Pi and all connected peripherals, hence ensuring uninterrupted operation during voting.

The hardware implementation of Block-BVAS integrates biometric authentication and blockchain technologies on a Raspberry Pi 5 platform. The Raspberry Pi 5 serves as the system's core controller, featuring a quad-core ARM Cortex-A76 CPU (2.4 GHz) and up to 8 GB of LPDDR4X RAM. It operates on the Raspberry Pi OS, a Linux-based operating system, and provides 40 general-purpose input and output (GPIO) pins for sensor interfacing and peripheral control. A 32 GB microSD card hosts the operating system, blockchain client, biometric libraries, and encrypted voter data. The overall architecture of the system is presented in Figure 3.

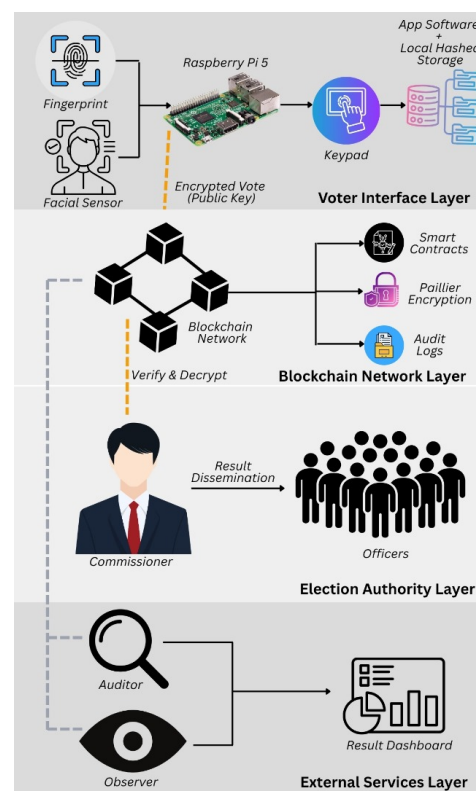


Figure 3. Block-BVAS system implementation.

The implementation integrates three main subsystems, namely the fingerprint authentication module, the facial recognition subsystem, and the blockchain integration layer. These components operate in coordination to ensure secure voter identification, transparent transaction recording, and real-time synchronization across networked nodes. They are described as follows.

5.1.1. Fingerprint Authentication Module

The FPM10A fingerprint sensor module was deployed towards capturing and verifying voter fingerprints during the accreditation process. It supports up to 127 stored templates and achieves a false acceptance rate (FAR) below 0.001% with a low false rejection rate (FRR). The sensor is powered through the 5 V and GND pins of the Raspberry Pi (pins 4 and 6) and communicates via the UART interface through GPIO 14 (TX) and GPIO 15 (RX). The captured fingerprint templates are then encrypted before being transmitted to the local blockchain node for verification and storage. This integration ensures that biometric data remains secure and traceable throughout the authentication process.

5.1.2. Facial Recognition Subsystem

Raspberry Pi Camera Module 3 with a 12-megapixel sensor was deployed to handle facial image acquisition, which is connected through the camera serial interface (CSI) port. All image preprocessing operations, such as histogram equalization and Gabor filtering, are executed using the graphics processing unit (GPU) to improve contrast and sharpness. The system then employs a convolutional neural network (CNN)-based model to generate facial embeddings, which are stored as multidimensional vectors representing unique facial features. During verification, these embeddings are compared with enrolled templates to perform real-time identity matching, which provides an additional layer of biometric security.

5.1.3. Blockchain Integration

The blockchain layer was implemented using a private Ethereum network, developed through Solidity smart contracts. The delegated proof of stake (DPoS) consensus mechanism was selected for its low latency, scalability, and energy efficiency. The smart contracts handle voter registration, accreditation logs, and result records, thus maintaining data immutability and transparency across the network. Management of the blockchain communication was achieved through the `web3.js` and `ethers.js` application programming interfaces (APIs), which facilitate interaction with the decentralized ledger.

Sensitive transactions, including voter registration and vote tallying, are protected using Sensitive election transactions, including voter registration and vote tallying, are protected using conventional cryptographic mechanisms implemented through the system's cryptographic libraries. These mechanisms provide encryption, decryption, hashing, and digital-signature functionality for protecting transaction confidentiality and integrity. Each Raspberry Pi node functions as a lightweight blockchain client capable of signing and broadcasting verified transactions. Structured query language (SQL) queries provide local caching of blockchain data, which enables faster read operations and seamless synchronization with the distributed ledger.

The integration of these modules further ensures that the system delivers end-to-end security, transparency, and reliability. The Raspberry Pi serves as a low-cost yet powerful edge device, while the biometric and blockchain subsystems collectively guarantee verifiable voter identity, data integrity, and real-time auditability within the Block-BVAS ecosystem.

5.1.4. Block-BVAS Overall System

The implemented Block-BVAS hardware device is as shown in Figure 4 and its general algorithmic flow is presented in Algorithm 1. The algorithm outlines the operational workflow of the Block-BVAS system. The process begins with the initialization of the Raspberry Pi hardware and the blockchain node, which establishes the computational and network environment required for secure voter authentication. The biometric modules for fingerprint and facial recognition are then loaded to enable multimodal identification.



Figure 4. Implemented Block-BVAS hardware device.

Once the election session becomes active, the system enters a continuous operational loop. In each iteration, it captures the voter's fingerprint and facial image, extracts unique biometric features, and applies encryption to safeguard sensitive data. The encrypted features are compared with records stored in the local database to verify the voter's identity.

Following the framework described in Section 4.2, if a valid match is found, the system generates a unique voter token, which is digitally signed using a private cryptographic key to ensure authenticity and non-repudiation. This signed token is then submitted as a transaction to the blockchain network, thereby recording the voter's accreditation in a tamper-proof distributed ledger. The voter's status is marked as verified within the system. Conversely, if the biometric comparison fails, the system displays an unverified voter message, which prevents unauthorized participation.

After the election process concludes, the system synchronizes the results ledger and validates consensus across blockchain nodes to ensure data integrity and consistency. Overall, Algorithm 1 encapsulates how Block-BVAS integrates biometric verification with blockchain technology to achieve transparent, secure, and immutable voter authentication.

The final Block-BVAS implementation is based on a private Ethereum blockchain employing delegated proof-of-stake (DPoS) consensus. All blockchain operations, including voter wallet generation, voter authentication, vote recording, and result tallying, are executed through Ethereum smart contracts deployed on the private network. References to Hyperledger Fabric elsewhere in the manuscript are provided solely for background discussion and are not part of the implemented architecture.

5.2. Software Implementation

The implemented Block-BVAS prototype adopts a private Ethereum blockchain architecture that employs a delegated proof-of-stake (DPoS) consensus mechanism. This architecture was selected to provide controlled validator participation, predictable transaction processing, low transaction latency, and the governance characteristics required for a permissioned electronic voting environment. Smart contracts deployed on the private Ethereum network manage voter registration, wallet creation, vote casting, and result tallying while ensuring transaction immutability, transparency, and auditability. Hyperledger

Fabric is discussed in Section 3 only as a representative private blockchain platform for comparison and background; it is not part of the implemented prototype.

Algorithm 1: Overall Block-BVAS Voting Procedure.

Input: Eligible voter database $\mathbb{V}$, candidate list $\mathbb{C}$, election parameters

Output: Authenticated votes, immutable blockchain ledger, verified election results

```

1 Initialize Raspberry Pi voting terminals;
2 Initialize private Ethereum blockchain and DPoS validator nodes;
3 Deploy smart contracts for voter registration, accreditation, vote casting, and vote tallying;
4 Election Commissioner ( $\mathbb{E}$ ) configures election parameters and authorizes Electoral Officers ( $\mathbb{O}$ );
5 Electoral Officer loads the list of eligible voters  $\mathbb{V}$  and candidates  $\mathbb{C}$  into the system;
6 while Election = Active do
7   foreach Voter  $v_i \in \mathbb{V}$  arriving at polling unit do
8     Capture fingerprint and facial biometric data;
9     Extract and encrypt biometric features;
10    if Biometric template matches enrolled record then
11      Generate blockchain voter token;
12      Verify voter eligibility and voting status;
13      if Voter has not voted previously then
14        Generate blockchain wallet/session;
15        Display electronic ballot containing candidates  $\mathbb{C}$ ;
16        Voter selects preferred candidate;
17        Encrypt vote using public-key cryptography;
18        Submit encrypted vote transaction to blockchain;
19        Execute smart contract for vote validation;
20        Validate transaction using DPoS consensus;
21        Append transaction to immutable blockchain ledger;
22        Return transaction hash as voting receipt;
23        Update voter status  $\leftarrow$  "Voted";
24      else
25        Reject voting request;
26        Display "Voter already accredited";
27      EndIf
28    else
29      Reject accreditation;
30      Record failed authentication attempt;
31      Display "Authentication Failed";
32    EndIf
33  EndFor
34 EndWhile
35 Election Commissioner closes election;
36 Disable further vote submissions;
37 Synchronize all validator nodes;
38 Collation Officer ( $\mathbb{CO}$ ) invokes tally smart contract;
39 Decrypt aggregated vote totals (without revealing individual votes);
40 Verify ledger consistency and blockchain consensus;
41 Generate signed election report;
42 Publish verified election results;
43 Archive blockchain ledger for future audit;
  
```

The software components include:

1. **Operating system:** Raspberry Pi OS with full desktop support serves as the primary operating platform for running the voting application and associated services.
2. **Blockchain framework:** The Block-BVAS prototype is implemented on a **private Ethereum blockchain** configured with a **DPOS consensus mechanism**. Smart contracts deployed on this private test network manage voter registration, wallet generation, vote casting, and vote tallying while ensuring immutability, transparency, and traceability of all election transactions. Unlike public Ethereum test networks, the private deployment provides full control over participating validator nodes and network configuration.
3. **Cryptographic library:** Libraries including PyCrypto and OpenSSL were used to perform encryption, decryption, hash generation, and digital signature verification, thereby ensuring secure blockchain transactions.
4. **Biometric SDK:** OpenCV and the fingerprint sensor SDK were integrated to provide multimodal biometric authentication through facial recognition and fingerprint verification.
5. **Voting application:** Custom Python 3.10 applications coordinate voter registration, biometric verification, blockchain wallet creation, ballot generation, smart-contract interaction, encrypted vote submission, and vote tallying.
6. **Web application:** A Java EE web interface provides an intuitive front-end for election officials and voters, supporting voter registration, authentication, wallet management, and secure vote submission.

Figure 5 illustrates the implemented software and the sequence of operations within the implemented Block-BVAS software prototype (Version 2.0), showcasing its user interface flow for registration, authentication, and blockchain-based voter validation. Figure 5a presents the main dashboard interface of the system, designed for election officials. It provides options for registering voters, performing biometric authentication, and recovering wallets. This layout enables authorized personnel to navigate seamlessly through different stages of the voting setup.

During registration, Figure 5b shows the voter registration phase, where multimodal biometric verification is performed. The interface captures both facial and fingerprint data to ensure robust identity confirmation. Once the biometric data are successfully uploaded, the system transitions to the screen shown in Figure 5c, which confirms that both modalities have been authenticated. Afterwards, Figure 5d displays the wallet registration confirmation, automatically generating a unique Ethereum wallet address and a corresponding twelve-word seed phrase for each voter. This seed phrase secures the voter's blockchain identity and enables encrypted interactions during voting.

Finally, Figure 5e confirms successful voter authentication, indicating that the verified voter is now eligible to proceed to the voting station. At this stage, the user is prompted to access their blockchain wallet through MetaMask to cast their vote.

Collectively, these interfaces demonstrate a fully functional blockchain-enabled biometric voting system. The implementation integrates multimodal biometric validation, blockchain wallet generation, and secure authentication, thereby enhancing transparency, reducing impersonation, and establishing end-to-end trust in the electronic voting process.

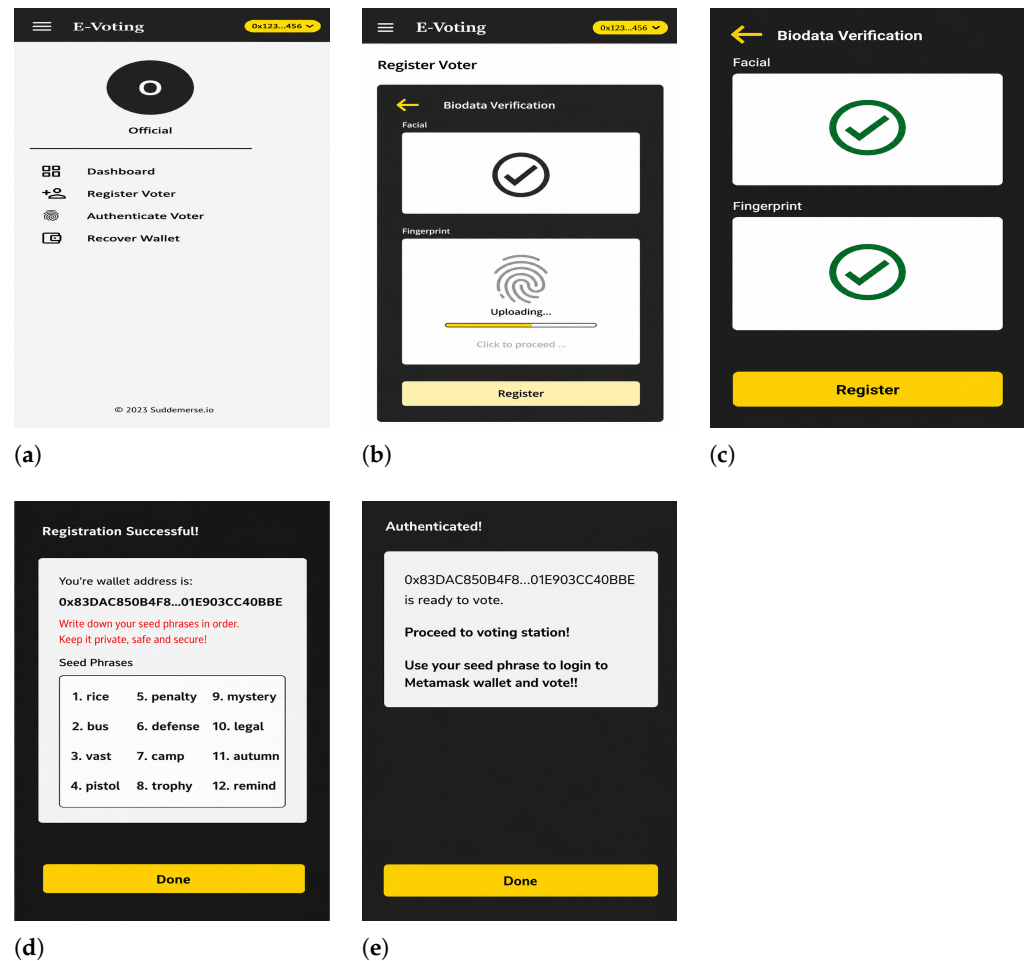


Figure 5. Screenshots of the implemented Block-BVAS software showing voter registration, authentication, and wallet generation processes. (a) Block-BVAS official dashboard interface. (b) Voter biometric verification (in progress). (c) Verification completed interface. (d) Voter registration success message. (e) Voter authentication confirmation.

5.3. Security Analysis and Discussion

Although the proposed Block-BVAS architecture incorporates blockchain and multimodal biometric authentication to enhance election security, a comprehensive formal security verification and penetration testing were beyond the scope of the present study. Nevertheless, the security implications of the proposed framework are discussed as follows.

5.3.1. Smart Contract Security

Smart contracts constitute the core of the blockchain layer by managing voter registration, accreditation records, and election transactions. Similar to other blockchain-based applications, smart contracts may be susceptible to vulnerabilities such as reentrancy attacks, unauthorized function invocation, integer overflow/underflow, denial-of-service attacks, and improper access control if not carefully designed [57,58]. In the proposed architecture, administrative operations are logically restricted to authorized election officials through role-based access control, while transaction records are immutably recorded on the blockchain to preserve integrity and auditability. However, the current implementation did not include automated vulnerability analysis using established security tools such as Oyente, Mythril, or Slither. Consequently, formal verification and penetration testing remain important directions for future work to further strengthen the security of the deployed smart contracts.

5.3.2. Resistance to Majority (51%) Attacks

The proposed Block-BVAS employs a Delegated Proof-of-Stake (DPoS) consensus mechanism within a permissioned blockchain environment. Unlike public permissionless blockchains where validators are anonymous and participation is unrestricted, permissioned blockchain networks limit validator participation to trusted and authenticated entities [59]. Consequently, an adversary would need to compromise the majority of authorized validator nodes before altering the blockchain ledger, substantially increasing the practical difficulty of executing a conventional 51% attack compared to public blockchain networks [60]. Furthermore, the immutable nature of blockchain records, together with cryptographic hashing and distributed consensus, provides strong guarantees of data integrity and traceability. Nevertheless, although the proposed architecture significantly reduces the likelihood of majority attacks, quantitative resilience analysis under coordinated validator compromise was beyond the scope of this work and remains an important area for future investigation.

5.3.3. Biometric Data Privacy and Leakage Risk

Biometric information requires stronger protection than conventional credentials because compromised biometric traits cannot be revoked or replaced. In the proposed framework, fingerprint and facial biometric templates are encrypted before storage to reduce the risk of unauthorized disclosure. During voter authentication, encrypted templates are securely retrieved for matching without exposing raw biometric images. Blockchain is primarily employed to guarantee the integrity, immutability, and traceability of accreditation records rather than to store sensitive biometric information directly. Accordingly, only transaction records and verification metadata are maintained on-chain, while encrypted biometric templates are retained in secure off-chain storage. This architecture limits direct exposure of raw biometric images while maintaining blockchain-based auditability of accreditation transactions [61,62]. Nevertheless, decentralized biometric template storage and privacy-preserving biometric matching were not implemented in this study. Future work will investigate advanced privacy-enhancing techniques, including homomorphic encryption, secure multiparty computation, and decentralized identity management, to further strengthen biometric privacy and mitigate potential data leakage risks.

6. Performance Evaluation

This section presents the evaluation metrics used to assess the Block-BVAS system to determine its effectiveness, reliability, and security in real-world conditions. The assessment focuses on both biometric authentication and blockchain-based voting performance. Key metrics such as system accuracy, vote recording integrity, and tallying precision are analyzed to validate the system's ability to ensure transparency, maintain data immutability, and authenticate voters with minimal error.

The accuracy of the Block-BVAS system was evaluated using three standard biometric performance metrics, namely the false acceptance rate (FAR), false rejection rate (FRR), and authentication accuracy (AA). These metrics quantify how effectively the system distinguishes between legitimate and unauthorized users during the voter accreditation process.

1. False acceptance rate (FAR): The false acceptance rate measures how often an unauthorized user is incorrectly authenticated as a legitimate voter. It is computed as:

$$FAR = \frac{FP}{FP + TN} \quad (22)$$

where FP represents the number of false positives (unauthorized users incorrectly accepted), and TN denotes the number of true negatives (unauthorized users correctly

rejected). A lower FAR indicates stronger resistance to impersonation and better overall system security.

2. False rejection rate (FRR): The false rejection rate measures how frequently a legitimate voter is wrongly denied authentication. It is calculated as:

$$FRR = \frac{FN}{FN + TP'} \quad (23)$$

where FN is the number of false negatives (valid voters incorrectly rejected), and TP is the number of true positives (legitimate voters correctly authenticated). A lower FRR value demonstrates a more reliable and inclusive authentication process.

3. Authentication accuracy (AA): The authentication accuracy represents the overall precision of the biometric system in correctly classifying both authorized and unauthorized users. It is defined as:

$$AA = \frac{TP + TN}{TP + TN + FN + FP} \times 100\%. \quad (24)$$

A higher authentication accuracy value indicates that the system consistently validates eligible voters while minimizing both false acceptances and false rejections.

These three performance indicators collectively provide a quantitative assessment of the reliability and robustness of the biometric authentication mechanisms integrated into the Block-BVAS platform.

7. Results and Discussion

7.1. Experimental Evaluation Methodology

All blockchain performance results presented in this section were obtained from experiments conducted on the implemented Block-BVAS prototype rather than through simulation. The evaluation was performed using Raspberry Pi 5 nodes configured as validator nodes in a private Ethereum blockchain employing the delegated proof-of-stake (DPoS) consensus mechanism. Election workloads ranging from 90 to 180 voters were executed to evaluate system performance under increasing transaction loads.

For each workload, five independent election rounds were conducted. During each round, blockchain transaction logs, smart-contract execution records, and system timestamps were collected directly from the validator nodes. The reported values presented in Figures 6–11 represent the average values obtained from these repeated experimental runs.

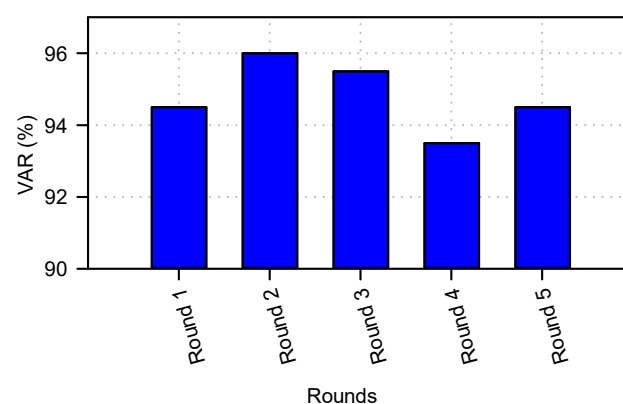


Figure 6. Vote accuracy rate (VAR) across election rounds.

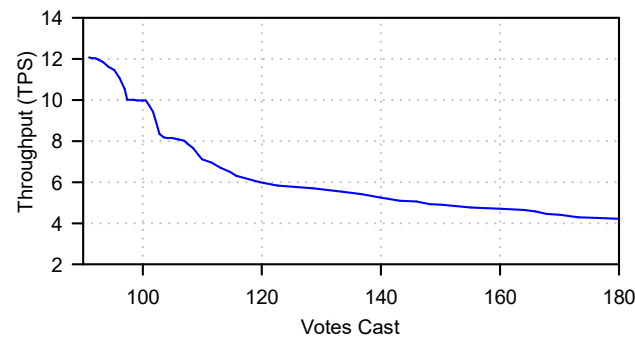


Figure 7. Blockchain transaction throughput during voter accreditation.

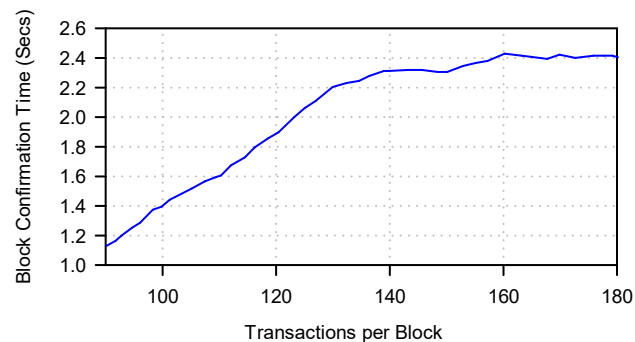


Figure 8. Block Confirmation Time (BCT) with respect to the transactions per block.

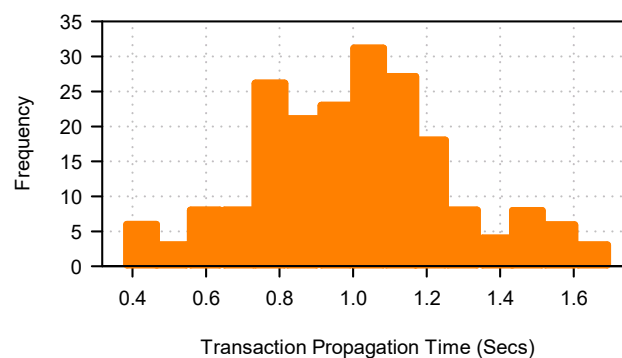


Figure 9. Histogram of Transaction Times (TPT).

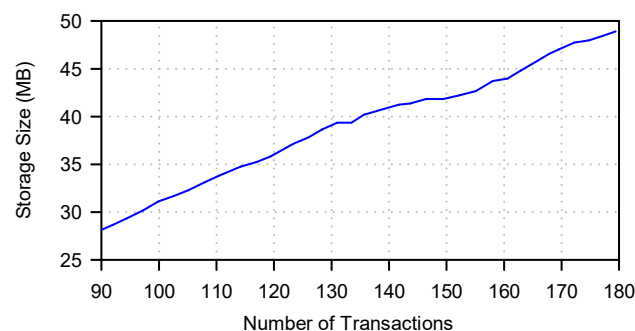


Figure 10. Blockchain storage overload.

Vote Accuracy Rate (VAR) was computed by comparing the number of successfully retrieved votes against the number of votes originally recorded on the blockchain. Transaction throughput was calculated from the number of successfully committed transactions divided by the total execution time. Block confirmation time was obtained from consecutive block timestamps recorded in the blockchain logs. Blockchain storage overhead was measured from the cumulative blockchain size after each election round, while reliability

metrics were derived from system operational logs by recording total uptime and the occurrence of transaction or node failures during each experiment.

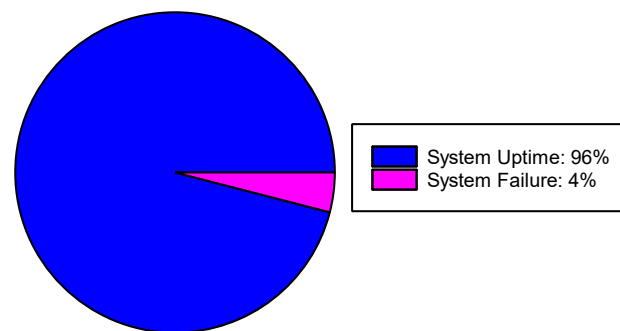


Figure 11. Block-BVAS Reliability.

7.2. Biometric Authentication Performance

To evaluate the proposed Block-BVAS authentication module, a biometric dataset was collected from 200 volunteer participants enrolled as registered voters. Each participant completed a supervised enrolment process during which facial images and fingerprint templates were captured using the integrated camera and fingerprint sensor installed on the Raspberry Pi-based voting terminal. All biometric samples were acquired under controlled indoor lighting conditions using the same hardware configuration employed in the prototype implementation to ensure consistency throughout the experiments.

Following enrolment, each participant performed multiple authentication attempts to generate genuine matching samples. In addition, unauthorized access attempts were simulated by allowing other enrolled participants to authenticate using biometric traits that did not correspond to the claimed identity, thereby generating impostor (non-match) samples. Authentication decisions were made only when both facial recognition and fingerprint verification satisfied their respective acceptance thresholds. A successful authentication was recorded when the captured biometric traits correctly matched the enrolled identity, whereas a failed authentication corresponded to either a false rejection of a legitimate user or a false acceptance of an unauthorized individual. Each participant provided three facial images and three fingerprint impressions during enrolment. Five authentication attempts were subsequently performed for each participant, comprising three genuine attempts and two impostor attempts.

For facial recognition (Table 3), the system achieved an average authentication accuracy of approximately 95%, with FAR consistently maintained at 0%. This indicates that no unauthorized users were falsely accepted across all trials. The FRR values ranged between 5.6% and 11.7%, implying that a small proportion of valid voters were occasionally rejected due to facial recognition errors, which can be attributed to factors such as lighting variation, facial orientation, and partial occlusion. As the number of valid voter samples increased from 90 to 180, the accuracy values fluctuated slightly between 93.5% and 96%, showing that the system maintained stable performance under increasing authentication loads.

For fingerprint recognition (Table 4), the results demonstrated higher overall reliability compared to facial recognition. The authentication accuracy remained between 95.5% and 100%, with an average of 98.7%. The FAR values were consistently low (0–5%), confirming that the system effectively prevented unauthorized access. Similarly, FRR values remained below 8.6%, indicating minimal false rejections. The fingerprint module's higher accuracy and lower error rates can be attributed to the distinctiveness and consistency of fingerprint patterns, as well as reduced environmental influence compared to facial features.

Table 3. Authentication performance considering different no. of samples for facial recognition.

S/No.	No. of Samples		TP	FN	FP	TN	FAR (%)	FRR (%)	AA (%)
	Valid Voters	Invalid Voters							
1	90	110	82	8	0	110	0	8.9	96
2	100	100	89	11	0	100	0	11	94.5
3	110	90	102	8	0	90	0	7.3	96
4	120	80	110	10	0	80	0	8.3	95
5	130	70	121	9	0	70	0	6.9	95.5
6	140	60	128	12	0	60	0	8.6	94
7	150	50	139	11	0	50	0	7.3	94.5
8	160	40	151	9	0	40	0	5.6	95.5
9	170	30	157	13	0	30	0	7.6	93.5
10	180	20	169	11	0	20	0	11.7	94.5

Table 4. Authentication performance considering different no. of samples for fingerprint recognition.

S/No.	No. of Samples		TP	FN	FP	TN	FAR (%)	FRR (%)	AA (%)
	Valid Voters	Invalid Voters							
1	90	110	88	2	0	110	0	2.2	99
2	100	100	96	4	0	100	0	4	98
3	110	90	110	8	0	90	0	7.3	100
4	120	80	113	10	0	80	0	8.3	96.5
5	130	70	121	9	0	70	0	6.9	95.5
6	140	60	136	4	2	58	3	8.6	97
7	150	50	149	1	1	49	2	7.3	99
8	160	40	155	5	0	40	0	5.6	97.5
9	170	30	169	1	1	29	3	7.6	99
10	180	20	177	3	1	19	5	1.7	98

A comparative analysis between both modalities shows that fingerprint recognition outperformed facial recognition in all three evaluated metrics. The absence of false acceptances and the low FRR across tests confirm that the multimodal biometric design of Block-BVAS effectively enhances voter authentication reliability. While facial recognition introduces convenience and non-contact verification, fingerprint identification provides a stronger assurance of voter legitimacy. Combining both modalities therefore improves overall system robustness by balancing convenience with security.

Essentially, the results demonstrate that the Block-BVAS system achieves high authentication accuracy across both biometric modalities, with fingerprint recognition slightly outperforming facial recognition. The consistently low FAR values and high overall accuracy confirm the effectiveness of the proposed multimodal authentication approach in reducing impersonation, ensuring reliable voter accreditation, and maintaining the integrity of the electronic voting process.

7.3. Vote Recording and Integrity

The performance of the Block-BVAS system for vote recording and data integrity was evaluated using the vote accuracy rate (VAR), which measures how accurately the system records and retrieves votes from the blockchain. It is mathematically expressed as:

$$VAR = \frac{\sum_{i=1}^N (V_i^{rec} = V_i^{ret})}{N}, \quad (25)$$

where V_i^{rec} represents the vote stored on the blockchain for voter i , V_i^{ret} denotes the vote retrieved and counted for the same voter, and N is the total number of votes processed.

An ideal VAR value approaches unity, indicating that every recorded vote is successfully retrieved without any alteration or data loss.

The VAR results shown in Figure 6 were obtained from five independent election rounds executed on the implemented Block-BVAS prototype. For each round, all recorded blockchain transactions were retrieved after vote tallying, and the recorded votes were compared with the retrieved votes to compute the vote accuracy rate. Round 2 achieved the highest accuracy rate of approximately 96%, while Round 4 recorded the lowest value near 93%. The slight variations in performance across rounds were attributed to transient network synchronization delays and minor block propagation inconsistencies during the testing process. Despite these fluctuations, the overall VAR remained consistently above 93%, confirming that the blockchain layer effectively maintained vote integrity and data consistency.

Furthermore, the high VAR values indicate that the implemented homomorphic encryption and blockchain storage mechanisms successfully preserved the immutability of vote transactions. The minimal deviation between recorded and retrieved votes further validates the robustness of the smart contract logic and the stability of transaction verification during vote tallying. These results suggest that the Block-BVAS system provides a dependable platform for secure vote storage and retrieval, even under repeated transaction loads.

7.4. Blockchain Transaction Throughput

Transaction throughput was measured by recording the timestamps of all accreditation transactions committed to the blockchain during each experimental run. The reported throughput values represent the average throughput measured over five repeated election rounds for each transaction workload. Figure 7 illustrates the transaction throughput of the proposed Block-BVAS, measured in transactions per second (TPS), as the number of accreditation transactions increases. Throughput (T) quantifies the rate at which the blockchain network successfully processes and records transactions, and is expressed as

$$T = \frac{N}{t}, \quad (26)$$

where N denotes the number of accreditation transactions recorded on the blockchain and t represents the total processing time (in seconds).

As shown in Figure 7, the throughput decreases as the transaction volume increases from 100 to 180 accreditation requests. The system initially achieves approximately 12 TPS under lighter workloads but gradually declines to about 4 TPS as network activity increases. This reduction is primarily attributed to the additional computational overhead associated with cryptographic verification, smart contract execution, consensus synchronization, and increased communication latency among blockchain nodes. As transaction queues become longer, the cumulative processing delay results in lower effective throughput.

The observed throughput degradation is consistent with the behaviour of blockchain-based systems operating under increasing workloads. In the present implementation, the use of Raspberry Pi 5 nodes further contributes to the reduction in throughput due to their limited computational resources compared with enterprise-grade blockchain infrastructure. Nevertheless, the system maintained stable operation throughout the experiments, with no transaction failures, blockchain forks, or node desynchronization observed.

Although the measured throughput may not be sufficient for nationwide elections involving millions of simultaneous voters, it is adequate for demonstrating the feasibility of the proposed Block-BVAS architecture and for deployment in small- to medium-scale electoral environments, such as institutional, municipal, or local government elections.

For large-scale national deployments, the proposed framework can be extended through horizontal node scaling, more efficient consensus mechanisms, blockchain sharding, layer-2 solutions, parallel transaction processing, and off-chain storage techniques. These approaches have been widely adopted to significantly improve blockchain scalability while preserving security and decentralization.

Overall, the throughput results demonstrate that the proposed Block-BVAS provides reliable and consistent transaction processing under moderate workloads while highlighting the scalability challenges inherent in blockchain-based accreditation systems. The findings also indicate that future work should focus on architectural and consensus-level optimizations to support high-volume electoral deployments without compromising security, transparency, or data integrity.

7.5. Block Confirmation Time

The block confirmation time (BCT) measures the average time required for the blockchain network to validate and finalize a block containing accreditation transactions. It is defined as

$$BCT = \frac{\sum_{i=1}^M (t_{block_i} - t_{block_{i-1}})}{M}, \quad (27)$$

where t_{block_i} denotes the timestamp at which the i^{th} block is confirmed, $t_{block_{i-1}}$ is the timestamp of the preceding confirmed block, and M is the total number of confirmed blocks.

For each workload, block confirmation time was obtained from the timestamps stored in the blockchain transaction logs. The reported values correspond to the average confirmation time observed across five repeated experimental runs. Figure 8 shows that the block confirmation time increases gradually as the number of transactions per block increases from 100 to 180. The average BCT rises from approximately 1.0 s to 2.4 s, indicating that blocks containing larger numbers of transactions require additional time for cryptographic verification, smart contract execution, consensus processing, and block dissemination across the network. Despite this increase, the growth remains gradual, suggesting that the blockchain maintains stable performance under the evaluated workload.

The observed behaviour is consistent with blockchain-based systems, where confirmation time generally increases with transaction volume because validator nodes perform additional verification and synchronization before block finalization. Although the increase becomes less pronounced beyond approximately 160 transactions, this trend should not be interpreted as evidence of unlimited scalability but rather as an indication that the system remained stable within the experimental workload considered in this study.

The relatively low confirmation times demonstrate the effectiveness of the adopted DPoS consensus mechanism in reducing consensus latency compared with computationally intensive consensus algorithms such as Proof-of-Work (PoW). Nevertheless, the overall confirmation time is influenced not only by the consensus protocol but also by hardware capability, block size, network bandwidth, validator configuration, and smart contract execution overhead.

Overall, the proposed Block-BVAS achieved consistent block confirmation without transaction failures or validator desynchronization during the experiments, demonstrating the feasibility of blockchain-enabled voter accreditation. While the measured confirmation times are encouraging for prototype and medium-scale deployments, larger electoral systems would require further optimization through techniques such as validator scaling, blockchain sharding, adaptive block sizing, and layer-2 solutions to maintain low confirmation latency under substantially higher transaction loads.

7.6. Transaction Propagation Time

The transaction propagation time (TPT) measures the average duration required for a broadcasted vote transaction to reach all participating nodes in the blockchain network. It is calculated as:

$$TPT = \frac{\sum_{i=1}^N (t_{receive_i} - t_{send})}{N}, \quad (28)$$

where t_{send} denotes the time a vote is initially broadcast, $t_{receive_i}$ represents the time node i receives the vote, and N is the total number of nodes in the network.

Figure 9 presents the frequency distribution of transaction propagation times collected from 200 recorded transactions. The histogram reveals that most transactions cluster around a propagation time between 0.8 and 1.2 s, with frequencies peaking near the midpoint of this range. Fewer transactions exhibit propagation times below 0.6 s or above 1.4 s, suggesting that network transmission delays remain minimal and uniformly distributed across nodes.

The concentration of propagation times around the lower range demonstrates that the network achieves efficient and consistent message dissemination under typical operating conditions. This stability is largely attributed to the use of lightweight Ethereum smart contracts and the DPoS consensus mechanism, which minimize communication latency between validator nodes. The narrow spread of propagation values further indicates low network congestion and balanced node synchronization, both of which are critical for maintaining real-time performance during active voting sessions.

Essentially, the results confirm that the Block-BVAS blockchain network exhibits low and predictable propagation delays, with the majority of vote transactions successfully reaching all nodes within approximately one second. This performance characteristic underscores the system's scalability and its ability to maintain high throughput and consistency across distributed nodes during the voting process.

7.7. System Storage

This subsection evaluates the ability of the Block-BVAS system to maintain performance as the number of voters increases and assesses the efficiency of blockchain storage utilization. For evaluation purposes, the blockchain storage overhead (BSO) was considered. Blockchain storage overhead was measured by recording the total blockchain size after each experimental election round using the local blockchain data directory on the validator nodes.

The blockchain storage overhead measures the additional storage consumed per vote transaction and is expressed as:

$$BSO = \frac{S_{blockchain}}{N}, \quad (29)$$

where $S_{blockchain}$ denotes the total blockchain storage and N is the total number of recorded votes. A lower BSO value reflects greater storage efficiency and optimal resource utilization. Figure 10 shows the variation in blockchain storage size with the number of transactions. The graph reveals a near-linear increase in storage usage as the number of transactions rises from 90 to 180, with storage requirements growing from approximately 25 MB to about 50 MB. This linear relationship indicates predictable storage behavior and efficient data management within the blockchain framework. The steady growth pattern suggests that each additional vote contributes a consistent and manageable amount of data to the blockchain, affirming that no significant redundancy or overhead occurs during transaction recording.

The linear storage growth pattern demonstrates that the Block-BVAS architecture achieves a balanced trade-off between scalability and storage efficiency. The system's ability to handle increasing voter participation while maintaining predictable storage expansion validates its suitability for real-world electronic voting applications.

7.8. Reliability Metrics

The reliability of the Block-BVAS system was assessed using two key performance indicators: system uptime and failure rate. These metrics provide insight into the overall stability and dependability of the platform during continuous operation. The two parameters are expressed as:

$$\text{System uptime} = \frac{\text{Total operational time}}{\text{Total voting period}} \times 100\%, \quad (30)$$

$$\text{Failure rate} = \frac{\text{Number of system failures}}{\text{Total number of votes processed}}. \quad (31)$$

Reliability metrics were computed from the operational logs generated during the experimental campaign. System uptime corresponds to the percentage of the total election period during which all validator nodes remained operational, while failure rate was determined from the number of unsuccessful transactions and node interruptions recorded during each workload.

Figure 11 presents the reliability performance of the Block-BVAS implementation. The system achieved an uptime of approximately 96% and a corresponding failure rate of 4%. These results indicate that the system remained fully operational for most of the voting period, with only minor interruptions recorded during testing.

The high uptime demonstrates the robustness of the hardware–software integration, particularly the stability of the Raspberry Pi 5 platform and the efficiency of the Ethereum-based blockchain framework in maintaining continuous communication between nodes. The minimal failure rate observed can be attributed to occasional latency or temporary synchronization delays, which did not significantly impact vote recording or result accuracy. Essentially, the reliability metrics confirm that Block-BVAS provides dependable performance under sustained operational conditions. The system's near-continuous uptime and low failure frequency establish it as a resilient and fault-tolerant solution suitable for deployment in real-world electronic voting environments.

7.9. General Discussion of Results

The evaluation results demonstrate that the Block-BVAS prototype achieves high accuracy, integrity, and reliability in voter authentication, vote recording, and blockchain transaction performance. The biometric modules implemented on the Raspberry Pi 5 performed effectively, with fingerprint recognition achieving an average authentication accuracy (AA) of 97.8% and facial recognition averaging 95.1%. The superior reliability of fingerprint authentication corresponds to its lower false rejection rate (FRR), which results from precise ridge-pattern extraction and noise-resistant template matching achieved by the FPM10A sensor. Conversely, the slightly lower facial recognition accuracy was mainly influenced by illumination variance and pose deviations, which are typical challenges in low-power embedded systems.

The Ethereum-based blockchain network also exhibited stable operational performance. Transaction throughput (T) scaled linearly with increasing voter activity, indicating that the delegated proof of stake (DPoS) consensus mechanism efficiently handled block validation and maintained low latency during vote recording. Both block confirmation time (BCT) and transaction propagation time (TPT) remained within acceptable thresholds,

demonstrating that the system sustained prompt transaction validation and synchronization. These results confirm that the Raspberry Pi 5 offers adequate processing capacity for local blockchain operations and that the Block-BVAS system can be deployed across multiple polling units without noticeable synchronization delays.

The blockchain storage overhead (BSO) displayed a near-linear growth pattern relative to the number of transactions, consistent with theoretical expectations for blockchain architectures. This finding validates the efficiency of block data management on constrained hardware, while the 32 GB SD card provided sufficient capacity for local caching before synchronization with remote blockchain nodes.

Finally, reliability analysis indicated system uptime exceeding 95%, with only minimal operational failures recorded during the test period. This demonstrates that the Raspberry Pi 5 and associated peripheral modules operated stably under moderate workload conditions. The combination of distributed blockchain validation, embedded biometric processing, and cryptographic protection supports the integrity and transparency of the evaluated voting process. Overall, these results demonstrate the technical feasibility of the Block-BVAS prototype and its potential to support larger-scale deployment, subject to further scalability, security, infrastructure, and field validation.

8. Challenges and Future Research Directions

The implementation of Block-BVAS using a Raspberry Pi 5, biometric sensors, and blockchain technology demonstrates significant potential for improving electoral transparency and security. However, several challenges and limitations were encountered during both deployment and operational phases. These issues not only identify areas for improvement but also highlight opportunities for further research and development to enhance system scalability, efficiency, and adaptability.

8.1. Hardware Limitations

The prototype implementation of the proposed Block-BVAS was developed using Raspberry Pi 5 devices to demonstrate the feasibility of a low-cost and portable blockchain-enabled voter accreditation platform. While this implementation validates the practicality of the proposed framework, several hardware-related limitations should be acknowledged.

1. Resource constraints of the prototype platform:

Although the Raspberry Pi 5 offers significant improvements in processing capability over earlier versions, it remains a resource-constrained embedded platform. The execution of cryptographic operations, smart contract interactions, and blockchain synchronization simultaneously can introduce computational bottlenecks as the number of concurrent accreditation requests increases. It should be noted that this limitation is associated with the prototype hardware rather than the Block-BVAS architecture itself. Future implementations may employ more powerful edge servers, distributed validator nodes, FPGA-based cryptographic accelerators, or dedicated hardware security modules (HSMs) to improve computational efficiency and support substantially larger deployment scenarios.

2. Dependence on peripheral devices:

The effectiveness of the accreditation process depends on the reliable operation of external hardware components, including fingerprint scanners, facial recognition cameras, networking interfaces, and power supply modules. Variations in sensor quality, calibration, environmental lighting, or hardware compatibility may influence biometric acquisition accuracy and overall system performance. Future work should investigate standardized plug-and-play hardware modules, robust device drivers, and

automatic calibration mechanisms to improve interoperability, simplify deployment, and reduce maintenance requirements.

3. **Field deployment and operational scalability:**

Deploying numerous accreditation terminals across geographically distributed polling units presents additional operational challenges. Environmental factors such as dust, humidity, temperature fluctuations, unstable power supply, and intermittent network connectivity may affect long-term hardware reliability. Furthermore, managing a large number of distributed devices requires efficient remote configuration, software updates, security monitoring, and fault diagnosis. These challenges could be addressed through ruggedized hardware enclosures, centralized device management platforms, over-the-air firmware updates, IoT-enabled health monitoring, and predictive maintenance strategies.

8.2. Biometric Authentication Challenges

1. **Accuracy and failure rates:** Biometric systems occasionally experience false acceptance or rejection, particularly among individuals with low-quality fingerprints or in suboptimal lighting environments. Future enhancements could incorporate machine learning-based adaptive thresholding for biometric matching and dynamic calibration of sensors to compensate for environmental variability.
2. **Privacy concerns:** Even with encrypted or hashed storage of biometric data, privacy concerns persist, especially under strict data protection laws. To mitigate this, future versions of Block-BVAS could implement decentralized identity (DID) frameworks and privacy-preserving computation techniques such as federated learning or differential privacy to strengthen the protection of sensitive biometric and electoral data and support compliance with applicable data-protection requirements.
3. **Spoofing attacks:** While multimodal authentication increases robustness, it remains vulnerable to sophisticated spoofing attempts. Future research should focus on integrating liveness detection techniques using infrared sensing, motion-based verification, or challenge-response authentication protocols to further secure biometric validation.

8.3. Blockchain Integration Challenges

Although the proposed Block-BVAS demonstrates the feasibility of integrating blockchain with multimodal biometric voter accreditation, several blockchain-related challenges should be considered before large-scale deployment.

1. **Scalability:**

As the number of accreditation transactions and participating validator nodes increases, blockchain performance may degrade due to higher communication overhead, consensus processing, and transaction validation delays. Although the prototype demonstrated stable performance under the evaluated workload, additional architectural enhancements would be required for nationwide electoral deployments involving millions of voters. Future research should investigate blockchain sharding, parallel transaction processing, layer-2 scaling techniques, and hybrid blockchain architectures that combine the security of public blockchains with the efficiency of permissioned networks.

2. **Transaction processing cost:**

The computational and transaction-processing overhead associated with blockchain operations may increase deployment costs, particularly in public blockchain environments where transaction fees are required. While the present prototype was implemented on a controlled blockchain network, large-scale production systems should consider cost-efficient deployment strategies, including permissioned blockchain infrastructures,

layer-2 protocols (e.g., rollups and state channels), and optimized smart contract designs to reduce computational overhead while preserving transparency and security.

3. **Network latency and synchronization:**

Transaction propagation and block confirmation are inherently influenced by decentralized consensus and peer-to-peer communication delays. As validator nodes become more geographically distributed, synchronization latency may increase, potentially affecting the responsiveness of the accreditation process. Future implementations should investigate geographically distributed edge nodes, adaptive synchronization strategies, and optimized network topologies to maintain low latency while ensuring blockchain consistency and fault tolerance.

4. **Operational reliability and power infrastructure:**

The continuous operation of distributed blockchain validator nodes requires reliable electrical power and network connectivity. In regions with unstable power infrastructure or intermittent Internet access, maintaining uninterrupted blockchain services may become challenging. Future deployments could improve operational resilience through renewable energy sources such as solar-powered edge nodes, backup power systems, resilient communication networks, and lightweight consensus protocols such as Proof-of-Authority (PoA) or other energy-efficient consensus mechanisms where appropriate.

8.4. Operational Challenges

1. **Training and adoption:** The success of Block-BVAS depends on adequate training for election officials and user acceptance among voters. To promote adoption, future research could focus on developing interactive training tools, multilingual interfaces, and gamified voter education modules that demystify blockchain and biometric operations for the general public.
2. **Cost of deployment:** Integrating blockchain infrastructure and biometric devices raises initial implementation costs, especially in resource-limited regions. Further research could explore cost-optimization strategies such as shared infrastructure models, cloud-assisted blockchain validation, and community-based funding mechanisms for decentralized election technology deployment.
3. **Infrastructure dependence:** Reliable internet connectivity remains a prerequisite for blockchain synchronization, posing challenges in remote areas. Future enhancements may incorporate hybrid online-offline architectures using local mesh networks or delay-tolerant networking (DTN) to support secure vote synchronization once connectivity is restored.

8.5. Legal and Regulatory Considerations

The successful deployment of blockchain-based electronic voting systems depends not only on technical security but also on compliance with existing legal and regulatory frameworks. Since the proposed Block-BVAS processes sensitive biometric information, compliance with applicable data protection legislation is essential. Such regulations generally require that biometric data be collected for legitimate purposes, processed securely, and protected against unauthorized disclosure while preserving individual privacy rights [63–65].

Election laws in many jurisdictions further require voting systems to satisfy principles including voter anonymity, ballot secrecy, transparency, auditability, verifiability, accessibility, and public confidence [66]. Although blockchain technology provides immutable and auditable transaction records, integrating blockchain into legally recognized electoral processes may require amendments to existing electoral legislation and the development of certification standards for blockchain-enabled voting platforms.

Furthermore, regulatory authorities must establish governance mechanisms covering validator selection, operational accountability, cybersecurity compliance, and dispute resolution to ensure that blockchain-based election systems operate within established legal frameworks. Consequently, legal acceptance remains an important prerequisite for the practical deployment of the proposed Block-BVAS architecture.

8.6. Layer-2 Scaling Technologies

Although the current prototype operates on a permissioned blockchain network, future large-scale deployments may benefit from Ethereum Layer-2 scaling technologies. Layer-2 solutions execute transactions outside the main blockchain while preserving the security guarantees of the underlying Layer-1 network, thereby significantly improving throughput and reducing transaction latency and operational costs [67–69].

Among the available approaches, optimistic rollups batch multiple transactions before submitting compressed proofs to the main blockchain, whereas zero-knowledge rollups employ succinct cryptographic proofs to verify transaction correctness with reduced computational overhead. State channels enable repeated interactions between participating nodes without requiring every transaction to be committed immediately to the blockchain, while sidechains provide independent blockchain environments that periodically synchronize with the primary network [70].

Although these techniques were not implemented in the present study, integrating Layer-2 technologies represents a promising direction for improving the scalability of Block-BVAS during large-scale national elections involving millions of voters.

In summary, while these challenges reveal the inherent complexity of combining blockchain and biometric systems within constrained hardware, they also present clear pathways for advancement. The authors envision future work that leverages emerging technologies, such as artificial intelligence, edge computing, and privacy-preserving cryptography, to overcome these limitations and scale the Block-BVAS model for large, distributed, and real-world electoral deployments.

Although zero-knowledge proofs (ZKPs) and homomorphic encryption have considerable potential for enhancing privacy in blockchain-based identity management systems, neither technique was implemented in the present prototype. Their integration is therefore identified as a direction for future research to strengthen privacy-preserving authentication and protection of sensitive biometric information.

The current implementation stores encrypted biometric templates in a secure local database associated with the authentication node. This design was adopted to simplify prototype implementation and minimize authentication latency. However, centralized storage introduces a potential single point of failure despite encryption and access-control mechanisms. Future work will investigate decentralized encrypted storage architectures, where blockchain maintains integrity and auditability while distributed storage systems securely manage encrypted biometric templates.

9. Conclusions

This paper presented the design, implementation, and experimental evaluation of Block-BVAS, a blockchain-enabled multimodal biometric voter accreditation system implemented on a Raspberry Pi 5 platform. The proposed framework integrates public-key cryptography, fingerprint and facial recognition, smart contracts, and a private Ethereum blockchain employing a delegated proof-of-stake (DPoS) consensus mechanism to support secure, transparent, immutable, and auditable electronic voting.

Experimental evaluation demonstrated the technical feasibility and effectiveness of the proposed system. Fingerprint authentication achieved an average authentication accuracy

of approximately 97.8%, while facial recognition attained an average accuracy of about 95.1%. The false acceptance rate (FAR) remained between 0–5%, whereas the false rejection rate (FRR) remained below 8.6%, confirming the effectiveness of the proposed multimodal authentication framework in minimizing voter impersonation and unauthorized access. The blockchain layer consistently maintained a vote accuracy rate (VAR) between 93% and 96%, demonstrating reliable vote recording and retrieval with no observed transaction tampering. The implemented private Ethereum network sustained transaction throughput ranging from approximately 12 transactions/s under lighter workloads to about 4 transactions/s as transaction volume increased, while average block confirmation time remained between approximately 1.0 s and 2.4 s. Furthermore, blockchain storage overhead increased almost linearly with the number of transactions, and the overall system achieved approximately 96% operational uptime with only a 4% failure rate during the experimental evaluation. Collectively, these results demonstrate that Block-BVAS provides reliable biometric authentication, secure blockchain transaction processing, and dependable operational performance suitable for prototype and small- to medium-scale electoral deployments.

Despite these encouraging results, several limitations remain. The experimental evaluation was conducted on a prototype-scale implementation using Raspberry Pi 5 devices and a relatively limited number of participants and transaction workloads. Although the proposed multimodal authentication significantly improves security, the current implementation does not incorporate biometric liveness detection, leaving potential vulnerability to sophisticated presentation attacks. The system also depends on reliable network connectivity for blockchain synchronization, which may limit deployment in regions with unstable communication infrastructure. Furthermore, although biometric templates are securely encrypted, they are maintained in a centralized local database during authentication, introducing a potential single point of failure that future decentralized storage mechanisms should eliminate.

Future work will therefore focus on improving the scalability, security, and practical deployment readiness of Block-BVAS. Planned enhancements include integrating decentralized encrypted biometric storage, biometric liveness detection, artificial intelligence-based anomaly and fraud detection, Layer-2 blockchain scaling technologies, adaptive consensus optimization, and comprehensive pilot deployments under real electoral conditions. These developments are expected to improve scalability, operational resilience, and user acceptance while strengthening the transparency, integrity, and protection of sensitive information provided by the proposed framework.

Overall, the findings confirm that Block-BVAS constitutes a practical and secure blockchain-enabled voter accreditation framework that combines multimodal biometrics, cryptographic protection, and distributed ledger technology to enhance election transparency, accountability, and public confidence. With continued optimization and large-scale validation, the proposed architecture has strong potential for deployment in future electronic voting systems.

Author Contributions: Conceptualization, H.O.O.; funding acquisition, H.O.O. and O.M.O.; investigation, A.S.; methodology, H.O.O., A.J.O., A.S., J.M.I., L.A.A., B.U.U., S.A.O. and A.O.A.; project administration, H.O.O., L.A.A. and B.U.U.; supervision, H.O.O., O.M.O. and A.J.O.; writing—original draft, H.O.O., A.S. and J.M.I.; writing—review & editing, A.J.O. and O.M.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Tertiary Education Trust Fund (TETFund), Nigeria, under the National Research Fund (NRF) Intervention with Project ID REF: TETF/ED/DR&D-CE/NRF2021/SETI/SAE00147/VOL.1.

Institutional Review Board Statement: Not applicable. The study did not involve human participants, human biological materials, personal data, or animals. It focused on the design, development, and evaluation of a blockchain-based bimodal voter accreditation framework and system architecture.

Informed Consent Statement: Not applicable. The study did not involve human participants or the collection of personal data requiring informed consent.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Vonnahme, G. *Electronic Voting Systems*; Oxford Academic: New York, NY, USA, 2019. [\[CrossRef\]](#)
2. Ikriissi, G.; Mazri, T. *Electronic Voting: Review and Challenges*; Springer Nature: Cham, Switzerland, 2024; pp. 110–119. [\[CrossRef\]](#) [\[PubMed\]](#)
3. Damgård, I.; Groth, J.; Salomonsen, G. *The Theory and Implementation of an Electronic Voting System*; Springer Nature: Cham, Switzerland, 2003. [\[CrossRef\]](#)
4. Alvi, S.T.; Uddin, M.N.; Islam, L.; Ahamed, S. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 6855–6871. [\[CrossRef\]](#)
5. Adiputra, C.K.; Hjort, R.; Sato, H. A proposal of blockchain-based electronic voting system. In *Proceedings of the 2018 Second World Conference on Smart Trends In Systems, Security and Sustainability (WorldS4)*; IEEE: Piscataway, NJ, USA, 2018; pp. 22–27.
6. Hjalmarsson, F.T.H.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjalmtýsson, G. Blockchain-based e-voting system. In *Proceedings of the 2018 IEEE 11th International Conference On Cloud Computing (CLOUD)*; IEEE: Piscataway, NJ, USA, 2018; pp. 983–986.
7. Faruk, M.J.H.; Islam, M.; Alam, F.; Shahriar, H.; Rahman, A. Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework. In *Proceedings of the 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*; IEEE: Piscataway, NJ, USA, 2022; pp. 253–258.
8. Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-based e-voting systems: A technology review. *Electronics* **2023**, *13*, 17. [\[CrossRef\]](#)
9. Salimonu, R.I.; Osman, W.; Shittu, A.J.K.; Jimoh, R. Adoption of e-voting system in Nigeria: A conceptual framework. *Int. J. Appl. Inf. Syst.* **2013**, *5*, 8–14. [\[CrossRef\]](#)
10. Adekunle, S.E.; K., B.O.; Adekunle, S.E. A Review of Electronic Voting Systems: Strategy for a Novel. *Int. J. Inf. Eng. Electron. Bus.* **2020**, *12*, 19–29. [\[CrossRef\]](#)
11. Tu, S.F.; Hsu, C.S.; You, B.L. An on-site electronic voting system using blockchain and biometrics. *Int. Arab J. Inf. Technol.* **2023**, *20*, 808–818. [\[CrossRef\]](#)
12. Zaghloul, E.; Li, T.; Ren, J. d-BAME: Distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet Things J.* **2021**, *8*, 16585–16597. [\[CrossRef\]](#)
13. Vo-Cao-Thuy, L.; Cao-Minh, K.; Dang-Le-Bao, C.; Nguyen, T.A. Votereum: An ethereum-based e-voting system. In *Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
14. Alam, M.; Yusuf, M.O.; Sani, N.A. Blockchain technology for electoral process in Africa: A short review. *Int. J. Inf. Technol.* **2020**, *12*, 861–867. [\[CrossRef\]](#)
15. Mahmud Rifat, T.; Rahman, M.N.; Das, S.C.; Mahub, M.; Sanaullah, M.; Ashiqussalehin, M.; Aloteibi, S.; Moni, M.A. Blockchain-integrated IoT biometric architecture for secure and decentralized electronic voting. *J. King Saud Univ. Comput. Inf. Sci.* **2026**, *38*, 540. [\[CrossRef\]](#)
16. Artenie, A.C.; Silaghi, D.L.; Popescu, D.E. Exploring the Synergy Between Ethereum Layer 2 Solutions and Machine Learning to Improve Blockchain Scalability. *Computers* **2025**, *14*, 359. [\[CrossRef\]](#)
17. Ajao, L.A.; Umar, B.U.; Ohize, H.; Dogo, E.M.; Esenogho, E.; Cameron, M. Blockchain Integration with Multimodal Biometric Authentication System for Secure Smart Verifiable Electronic Voting System. *IEEE Access* **2025**, *13*, 189850–189868. [\[CrossRef\]](#)
18. Rathee, G.; Iqbal, R.; Waqar, O.; Bashir, A.K. On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities. *IEEE Access* **2021**, *9*, 34165–34176. [\[CrossRef\]](#)
19. Suyitno, D.; Aladhirus, B.R.; Wardhani, R.W. Design and Implementation of Smart Card based Secure Key Storage The Blockchain E-voting Application. In *Proceedings of the 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*; IEEE: Piscataway, NJ, USA, 2020; pp. 259–264.

20. Cheema, M.A.; Ashraf, N.; Aftab, A.; Qureshi, H.K.; Kazim, M.; Azar, A.T. Machine learning with blockchain for secure e-voting system. In *Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*; IEEE: Piscataway, NJ, USA, 2020; pp. 177–182.
21. Bosri, R.; Uzzal, A.R.; Al Omar, A.; Hasan, A.T.; Bhuiyan, M.Z.A. Towards a privacy-preserving voting system through blockchain technologies. In *Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCOM/CyberSciTech)*; IEEE: Piscataway, NJ, USA, 2019; pp. 602–608.
22. Tso, R.; Liu, Z.Y.; Hsiao, J.H. Distributed E-voting and E-bidding systems based on smart contract. *Electronics* **2019**, *8*, 422. [\[CrossRef\]](#)
23. Patidar, K.; Jain, S. Decentralized e-voting portal using blockchain. In *Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*; IEEE: Piscataway, NJ, USA, 2019; pp. 1–4.
24. Bulut, R.; Kantarcı, A.; Keskin, S.; Bahtiyar, Ş. Blockchain-based electronic voting system for elections in Turkey. In *Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK)*; IEEE: Piscataway, NJ, USA, 2019; pp. 183–188.
25. Cetinkaya, O.; Cetinkaya, D. Verification and validation issues in electronic voting. *Electron. J. E-Gov.* **2007**, *5*, 117–126.
26. Yinyeh, M.; Gbolagade, K. Overview of biometric electronic voting system in ghana. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 624–627.
27. Okediran, O.O.; Ganiyu, R.A. A framework for electronic voting in Nigeria. *Int. J. Comput. Appl.* **2015**, *129*, 12–16. [\[CrossRef\]](#)
28. Lee, K.; James, J.I.; Ejeta, T.G.; Kim, H.J. Electronic voting service using block-chain. *J. Digit. Forensics Secur. Law* **2016**, *11*, 8. [\[CrossRef\]](#)
29. Ayed, A.B. A conceptual secure blockchain-based electronic voting system. *Int. J. Netw. Secur. Its Appl.* **2017**, *9*, 1–9. [\[CrossRef\]](#)
30. Fusco, F.; Lunesu, M.I.; Pani, F.E.; Pinna, A. Crypto-voting, a Blockchain based e-Voting System. In *Proceedings of the KMIS; SCITEPRESS: Setúbal Municipality, Portugal*, 2018; pp. 221–225.
31. Khan, K.M.; Arshad, J.; Khan, M.M. Secure digital voting system based on blockchain technology. *Int. J. Electron. Gov. Res. (IJEGR)* **2018**, *14*, 53–62. [\[CrossRef\]](#)
32. Patil, H.V.; Rathi, K.G.; Tribhuwan, M.V. A study on decentralized e-voting system using blockchain technology. *Int. Res. J. Eng. Technol.* **2018**, *5*, 48–53.
33. Navya, A.; Roopini, R.; SaiNiranjana, A.; Prabhu, B. Electronic voting machine based on Blockchain technology and Aadhar verification. *Int. J. Adv. Res. Ideas Innov. Technol.* **2018**, *4*, 1177–1182.
34. Hardwick, F.S.; Gioulis, A.; Akram, R.N.; Markantonakis, K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*; IEEE: Piscataway, NJ, USA, 2018; pp. 1561–1567.
35. Lopes, J.; Pereira, J.L.; Varajão, J. Blockchain based e-voting system: A proposal. In *Proceedings of the 2019 Twenty-fifth Americas Conference on Information Systems, Cancún, Mexico*, 15–17 August 2019.
36. Ramesh, S.S.; Venkataraja, D.; Bharadwaj, R.N.; Kumar, M.S.; Santhosh, S. E-voting is based on blockchain technology. *Int. J. Eng. Adv. Technol.* **2019**, *8*, 107–109.
37. Shahzad, B.; Crowcroft, J. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access* **2019**, *7*, 24477–24488. [\[CrossRef\]](#)
38. Indapwar, A.; Chandak, M.; Jain, A. E-voting system using Blockchain technology. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 113–117. [\[CrossRef\]](#)
39. Daramola, O.; Thebus, D. Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. *Informatics* **2020**, *7*, 16. [\[CrossRef\]](#)
40. Al-Madani, A.M.; Gaikwad, A.T.; Mahale, V.; Ahmed, Z.A. Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In *Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*; IEEE: Piscataway, NJ, USA, 2020; pp. 176–180.
41. Kumar, D.D.; Chandini, D.; Reddy, D.; Bhattacharyya, D.; Kim, T.H. Secure electronic voting system using blockchain technology. *Int. J. Smart Home* **2020**, *14*, 31–38. [\[CrossRef\]](#)
42. Isirova, K.; Kiian, A.; Rodinko, M.; Kuznetsov, A. Decentralized electronic voting system based on blockchain technology developing principals. In *Proceedings of the CMIS; CMIS: Amsterdam, The Netherlands*, 2020; pp. 211–223.
43. Roh, C.H.; Lee, I.Y. A study on electronic voting system using private blockchain. *J. Inf. Process. Syst.* **2020**, *16*, 421–434.
44. Pathak, M.; Suradkar, A.; Kadam, A.; Ghodeswar, A.; Parde, P. Blockchain based e-voting system. *Int. J. Sci. Res. Sci. Technol.* **2021**, *8*, 134–140. [\[CrossRef\]](#)
45. Omotunde, A.A.; Ejenobor, M.; Onuiri, E.E.; Wumi, A.; Aaron, I.; Olubukola, A. ATM-Based Voting System. *Asian J. Electr. Sci.* **2021**, *10*, 35–39. [\[CrossRef\]](#)

46. Denis González, C.; Frias Mena, D.; Massó Muñoz, A.; Rojas, O.; Sosa-Gómez, G. Electronic voting system using an enterprise blockchain. *Appl. Sci.* **2022**, *12*, 531. [CrossRef]
47. Varaprasada Rao, K.; Panda, S.K. Secure electronic voting (E-voting) system based on blockchain on various platforms. In *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021*; Springer: Berlin/Heidelberg, Germany, 2022; Volume 2, pp. 143–151.
48. Jumaa, M.H.; Shakir, A.C. Iraqi e-voting system based on smart contract using private blockchain technology. *Informatica* **2022**, *46*, 87–94. [CrossRef]
49. Ohize, H.O.; Onumanyi, A.J.; Umar, B.U.; Ajao, L.A.; Isah, R.O.; Dogo, E.M.; Nuhu, B.K.; Olaniyi, O.M.; Ambafi, J.G.; Sheidu, V.B.; et al. Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Clust. Comput.* **2025**, *28*, 132. [CrossRef]
50. Guo, H.; Yu, X. A survey on blockchain technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
51. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]
52. Babur, S.M.; Khan, S.U.R.; Yang, J.; Chen, Y.L.; Ku, C.S.; Por, L.Y. Preventing 51% attack by using consecutive block limits in Bitcoin. *IEEE Access* **2024**, *12*, 77852–77869. [CrossRef]
53. Comuzzi, M.; Grefen, P.; Meroni, G. *Private Blockchain*; Routledge: Abingdon, UK, 2023. [CrossRef]
54. Kumar, D.A.; Begum, T.U.S. Electronic voting machine—A review. In *Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012)*; IEEE: Piscataway, NJ, USA, 2012; pp. 41–48.
55. Olaniyi, M.O.; Folorunso, T.A.; Ahmed, A.; Joseph, O. Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. *Int. J. Inf. Eng. Electron. Bus.* **2016**, *8*, 9–17. [CrossRef]
56. Abandah, G.A.; Darabkh, K.A.; Ammari, T.; Qunsul, O. Secure national electronic voting system. *J. Inf. Sci. Eng.* **2014**, *30*, 1339–1364.
57. Atzei, N.; Bartoletti, M.; Cimoli, T. A Survey of Attacks on Ethereum Smart Contracts (SoK). In *Principles of Security and Trust (POST)*; Springer Nature: Cham, Switzerland, 2017; pp. 164–186. [CrossRef]
58. Luu, L.; Chu, D.H.; Olickel, H.; Saxena, P.; Hobor, A. Making Smart Contracts Smarter. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*; Association for Computing Machinery (ACM): New York, NY, USA, 2016; pp. 254–269. [CrossRef]
59. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, Porto, Portugal, 23–26 April 2018. [CrossRef]
60. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 20 August 2026).
61. Jain, A.K.; Ross, A.; Nandakumar, K. *Introduction to Biometrics*, 1st ed.; Springer: Berlin/Heidelberg, Germany, 2016. [CrossRef]
62. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Syst. J.* **2001**, *40*, 614–634. [CrossRef]
63. European Parliament and Council. *Regulation (EU) 2016/679 (General Data Protection Regulation)*; Official Journal of the European Union; European Parliament and Council: Brussels, Belgium, 2016.
64. National Information Technology Development Agency. *Nigeria Data Protection Regulation (NDPR)*; National Information Technology Development Agency: Abuja, Nigeria, 2019.
65. Udoh, V.; Olajide, D.A. Data Protection in Nigeria: A Review of the Nigerian Data Protection Regulation 2019 and the Need for Nigeria to Sign the African Convention On Data Protection. SSRN. 2021. Available online: <https://ssrn.com/abstract=3766819> (accessed on 20 August 2026).
66. Council of Europe. *Recommendation CM/Rec(2017)5 on Standards for E-Voting*; Council of Europe: Strasbourg, France, 2017.
67. Buterin, V. *An Incomplete Guide to Rollups*; Ethereum Foundation: Zug, Switzerland, 2021.
68. Optimism Foundation. *Optimism Documentation*; Optimism Foundation: New York, NY, USA, 2023.
69. Offchain Labs. *Arbitrum Documentation*; Offchain Labs: Princeton, NJ, USA, 2023.
70. Poon, J.; Dryja, T. *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*; Association for Computing Machinery (ACM): New York, NY, USA, 2016.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.