JWP (Jurnal Wacana Politik)
ISSN 2502 - 9185 : E-ISSN: 2549-2969
Vol. 11, No. 1, January 2026: 116 - 125

BLOCKCHAIN ADOPTION IN THAILAND'S ELECTIONS: PERSPECTIVES, LIMITATIONS, AND THE PROPOSED TBERM MODEL

Charm Peeraphirom[1] and Waiwit Chanwimalueng[2]*
[1]Master of Science Program in Digital Innovation Management (Internet-based Distance Education), College of Digital Technology Innovation, Rangsit University, Pathum Thani, Thailand
[2]College of Digital Technology Innovation, Rangsit University, Pathum Thani, Thailand
Corresponding author: charm.p66@rsu.ac.th ; *waiwit.c@rsu.ac.th

ABSTRACT. This study assesses Thailand's readiness for blockchain-based elections by utilizing qualitative methods and semi-structured interviews with five experts in law, technology, economics, and administration. The data were analyzed through the dimensions of privacy, accessibility, transparency, security, and scalability. Findings reveal that while blockchain enhances integrity, significant barriers exist including insufficient transaction throughput, high costs, voter coercion risks, and limited digital literacy. Legal gaps regarding the PDPA also hinder adoption. Consequently, the study proposes the Thailand Blockchain Election Readiness Model (TBERM) which is a hybrid framework integrating blockchain auditing with physical polling units to mitigate security and accessibility concerns. The results indicate that Thailand is not yet prepared for full nationwide adoption but can transition through the proposed TBERM. The study recommends incremental implementation via pilot projects supported by legal reforms and public education.

Keywords: Blockchain; Election Readiness; TBERM; Hybrid Voting; Thailand

INTRODUCTION

Participation in elections is the cornerstone of democracy and a vital mechanism for citizens to express their opinions in shaping national governance. Such participation reflects civic responsibility and serves as the foundation for transparent and sustainable politics (Mannonov & Myeong, 2024). It ensures the selection of capable representatives and policies that align with social needs. These representatives play a crucial role in legislative processes and public policy formulation, which are essential for national development.

However, traditional electoral systems continue to face several limitations, including risks of corruption, human error, lack of transparency, and limited accessibility for certain population groups. Furthermore, the high operational costs associated with personnel and logistics remain a significant challenge (El Kafhali, 2024). These issues frequently lead to public skepticism regarding the efficiency and integrity of the electoral process.

To address these challenges, blockchain technology has emerged as a promising solution. Its core characteristics—security, transparency, and real-time auditability—offer significant potential to enhance the electoral process (Benabdallah et al., 2022). The immutable nature of blockchain prevent retroactive data manipulation, while smart contracts enhance the reliability of key processes such as voting, user authentication, and ballot counting (Pereira et al., 2023).

Additionally, remote electronic voting can facilitate greater accessibility for voters, reducing constraints related to time and travel while minimizing human errors caused by fatigue during the manual counting process.

Despite its high potential, the practical implementation of blockchain still faces several hurdles, including the readiness of digital infrastructure, cybersecurity threats, the design of standardized protocols, and the need to bridge the digital divide (Kothari et al., 2025). Therefore, careful planning, in-depth research, and governmental support are vital for the successful integration of blockchain into electoral systems.

This research aims to explore the feasibility of applying blockchain technology to the electoral system in Thailand. The study examines blockchain's potential in ensuring data integrity, preventing fraud, providing real-time auditability, and promoting accessibility through electronic devices (Çabuk et al., 2018). The goal is to develop an effective framework for future digital election systems in Thailand.

Key Evaluation Dimensions

To evaluate the readiness of Thailand for the implementation of blockchain technology within its national electoral processes, this research establishes a conceptual framework centered on five fundamental evaluation dimensions. These dimensions encompass privacy, accessibility, transparency, security, and scalability. The rationale for selecting this specific framework is to ensure a multi-dimensional and comprehensive analysis that effectively covers both technical infrastructures and broader social perspectives. Furthermore, this approach aligns with a substantial body of academic literature which suggests that these five factors serve as

DOI: https://doi.org/10.24198/jwp.v11i1.68023
Submited: 12 November 2025, Accepted: 22 January 2026, Publish: 26 January 2026

the primary pillars for designing and auditing blockchain-based voting architectures. Whether the system is categorized as public, private, or hybrid, each model exhibits varying levels of operational transparency and data security. This methodological approach also builds upon several influential previous studies that emphasize the critical importance of these five dimensions in the rigorous analysis of digital voting systems (Çabuk et al., 2018; El Kafhali, 2024; Singh et al., 2023).

An Innovation with Potential to Transform Electoral Systems

Blockchain, or distributed ledger technology (DLT), has an operational structure as shown in Figure 1, which illustrates the linkage of data blocks and data encryption. This technology is designed to enhance data transparency and credibility. By distributing control across multiple computers in a network, blockchain makes tampering difficult and reduces concerns regarding user security and privacy (Benabdallah et al., 2022; Deviani, 2023; El Kafhali, 2024). Every transaction must undergo a consensus process to achieve agreement among network participants before being stored in the system (Benabdallah et al., 2022; Berenjestanaki et al., 2023).

Through permanent data recording and chain-like linkage, blockchain possesses immutable properties against retrospective modification and enables traceability. These characteristics make blockchain a suitable technology for addressing the limitations of traditional electoral systems in terms of transparency, security, and privacy (Benabdallah et al., 2022; Sahib & Al-Shamery, 2021).

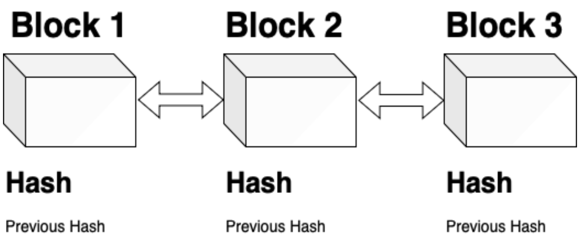

Figure 1. Blockchain operation process

In addition to consensus mechanisms, blockchain relies on encryption using the SHA-256 algorithm to process inputs into a fixed-size 256-bit hash value, regardless of the input size (Benabdallah et al., 2022; Singh et al., 2023). SHA-256 ensures data integrity and prevents modification or forgery, as reversing the hash value back to the original data is practically impossible (Singh et al., 2023). This process is illustrated in Figure 2.

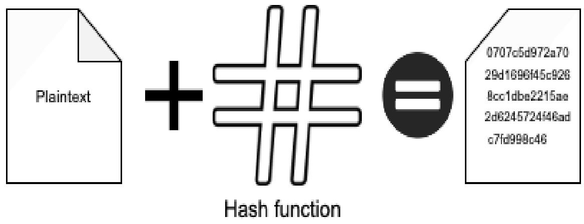

Figure 2. SHA-256 cryptographic process

Capabilities of Blockchain in the Context of Electoral Systems

To evaluate the potential of blockchain technology for implementation in electoral systems, this research applies a five-dimensional analysis framework: Privacy, Accessibility, Transparency, Security, and Scalability. These dimensions have been proposed and supported by numerous studies regarding blockchain-based voting systems.

Privacy

Blockchain can significantly enhance voter privacy through data encryption and the decoupling of identity from voting transactions. Consequently, voters cannot be directly identified from the data recorded in the system. Additionally, Zero-Knowledge Proofs (ZKP) technology helps verify the validity of a vote without requiring the disclosure of the voter's personal information, allowing blockchain to maintain both confidentiality and data integrity simultaneously (Deviani, 2023; El Kafhali, 2024; Mukherjee et al., 2023; Singh et al., 2023). The work of Mukherjee et al. (2023) emphasizes that employing these advanced cryptographic techniques is key to maintaining privacy in decentralized electoral systems like blockchain.

Accessibility

Blockchain-based electoral systems can greatly reduce geographical and physical mobility constraints for citizens. Voters can cast their ballots from anywhere via internet-connected devices, which increases public participation, particularly for remote groups or those with limitations (Deviani, 2023; El Kafhali, 2024). Furthermore, the work of Khaldun (2025) indicates that expanding access through online systems can strengthen civic engagement at the national level.

Transparency

Blockchain enhances transparency in the electoral process, as data recorded on the blockchain is immutable and traceable. These are essential properties that increase transparency at every stage of the election process (Benabdallah et al., 2022; Çabuk et al., 2018; Choi et al., 2021; El Kafhali, 2024; Berenjestanaki et al., 2023; Pereira et al., 2023).

Security

One of the primary strengths of blockchain is its ability to resist data tampering and cyber-attacks. This results from the use of a decentralized structure and various consensus mechanisms, such as Proof of Work or Proof of Stake (Daramola & Thebus, 2020; Deviani, 2023; Singh et al., 2023). The study by Singh et al. (2023) highlights that blockchain offers a high level of security because recorded data is protected by hash functions like SHA-256, making retrospective data modification virtually impossible.

Scalability

Although the strengths in security and transparency make blockchain attractive for elections, the capability to support a massive volume of transactions within a short timeframe remains a significant challenge for national-level implementation (El Kafhali, 2024). It is stated that "blockchain-based voting systems need the capability to support many voters simultaneously and provide opportunities to cast votes whenever desired.

Essential Mechanisms in Blockchain Systems for Elections

To ensure that a blockchain-based election operates with the required integrity and efficiency, several core technical components must work in tandem. Among these, consensus mechanisms and smart contracts are the most fundamental elements that transform a simple distributed ledger into a robust, automated, and trustless electoral infrastructure. These mechanisms provide the technical foundation for decentralized validation and the autonomous execution of voting rules, as detailed below.

Consensus mechanisms

Consensus mechanisms are critical components of blockchain that enable all computers in the network to verify transactions and reach a mutual agreement on the latest data state without relying on a central authority (Çabuk et al., 2018). This mechanism provides blockchain with reliability, transparency, and resistance to attacks due to its Byzantine Fault Tolerance (BFT) property. This allows the system to continue functioning correctly even if some computers fail or are controlled by malicious actors (Benabdallah et al., 2022).

Widely used examples of consensus mechanisms include Proof of Work (PoW), which relies on computational power to solve mathematical problems for verifying new blocks. While PoW offers high security and is difficult to attack, it consumes significant energy and has low processing speeds (Berenjestanaki et al., 2023). In contrast, Proof of Stake (PoS) uses the proportion of tokens held by users as the criterion for granting block validation rights. This reduces energy consumption and increases system speed but carries a risk of power centralization among large token holders (Berenjestanaki et al., 2023).

When applied to electoral systems, consensus mechanisms ensure that every transaction—such as voting, identity verification, and vote counting—must be confirmed by the network before being recorded on a block. Consequently, the data remains transparent, traceable, and resistant to tampering, allowing citizens to confidently trust the recorded election results (Çabuk et al., 2018; El Kafhali, 2024; Reddy et al., 2021).

Smart Contracts

Smart Contracts are digital programs stored and executed automatically on the blockchain when predefined conditions are met. This mechanism reduces reliance on intermediaries, enhances operational accuracy, and mitigates the risk of interference or data modification (Singh et al., 2023).

In the context of blockchain-based electoral systems, smart contracts can be utilized to verify voter eligibility, such as checking whether a digital wallet address has already exercised its voting right, thereby guaranteeing the "one person, one vote" principle (Choi et al., 2021). Votes submitted to the system are encrypted and permanently recorded on the blockchain, making them immutable and verifiable at every stage. This results in increased accuracy, reliability, and transparency of the election results (El Kafhali, 2024; Pereira et al., 2023).

Evolution of Electoral Processes: From Traditional Systems to the Blockchain Revolution

Blockchain is viewed as a high-potential technology for privatizing electoral systems by addressing critical limitations of traditional systems, such as lack of transparency, risks of data tampering, human error, and high administrative costs. The core properties of blockchain **including** privacy, accessibility, transparency, and security support the creation of a more auditable, transparent, and reliable election system. This is particularly effective when integrated with cryptographic techniques and smart contracts that automatically verify eligibility and record votes (Deviani, 2023; Pereira et al., 2023). The ability of blockchain to prevent data modification and create an audit trail makes this technology highly suitable for national elections that demand high levels of accuracy, precision, and public trust (El Kafhali, 2024; Sahib & Al-Shamery, 2021).

The blockchain-based voting process

Begins with the voter registration stage, which may be conducted through official government documents, biometric data, or digital identity verification systems such as e-KYC or NDID. Once identity verification is complete, the system generates a user account linked to a digital key pair. All registration data is encrypted and recorded on the blockchain in an immutable format (Çabuk et al., 2018; Choi et al., 2021).

On election day, the system issues digital ballots in the form of tokens to eligible voters. Voters use their private keys to log into the system and select candidates. This stage may be managed through smart contracts, which function to verify eligibility, prevent double voting, and automatically record votes. Each voting record is stored as a new transaction on the blockchain and is confirmed by the consensus mechanism before being permanently recorded in the subsequent block (Deviani, 2023; Benabdallah et al., 2022).

Following the vote, the system records and confirms votes in real-time. Voters can verify the status of their ballots to ensure they were recorded accurately and without alteration. Meanwhile, the vote counting and result announcement systems operate automatically through smart contracts, providing fast, accurate, and transparent results while maintaining voter privacy (El Kafhali, 2024; Berenjestanaki et al., 2023; Pereira et al., 2023).

The overview of the blockchain election process is illustrated in Figure 3, showing the sequence from identity verification, digital token issuance, and voting via smart contracts, to consensus processing, auditing, and the transparent announcement of results on the blockchain network.

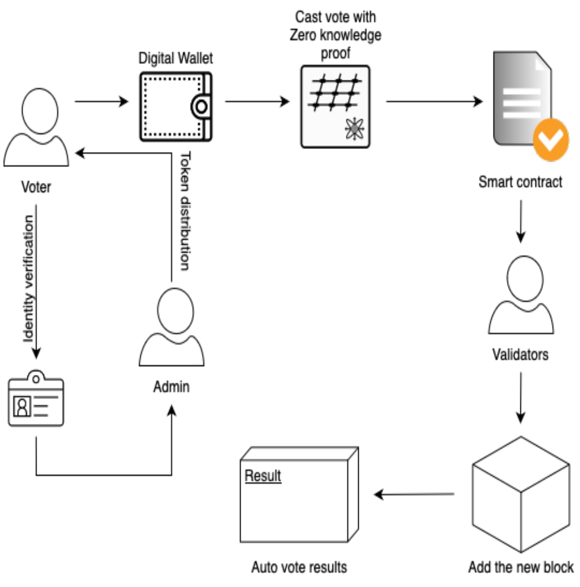

Figure 3. Blockchain-based election process

Traditional election systems

Begin with voter registration, which must be completed in advance with relevant authorities, such as the Election Commission. Voter data is stored in a centralized database for identity verification on election day. In Thailand, voters must present their national identification cards to verify their identity before receiving a ballot. The voting process involves marking a paper ballot and dropping it into a ballot box at a polling station. After the polls close, the ballots are transported to a central counting center, a stage that requires significant manpower and carries risks of error or interference during transit (Sahib & Al-Shamery, 2021).

The counting process utilizes manual methods, which demand high precision and are time-consuming, especially in national elections with many voters. Traditional systems also face several limitations, such as public distrust, a lack of data transparency for auditing, high costs for personnel and logistics, delayed reporting of results, and the risk of human error, all of which can affect the overall credibility of the election results (Berenjestanaki et al., 2023; El Kafhali, 2024).

Figure 4 illustrates the sequence of the traditional election process, starting from registration, list verification, ballot issuance, marking in the voting booth, and dropping the ballot into the box, to the transportation and manual counting after the polls close. This entire process is susceptible to delays and errors at every stage.

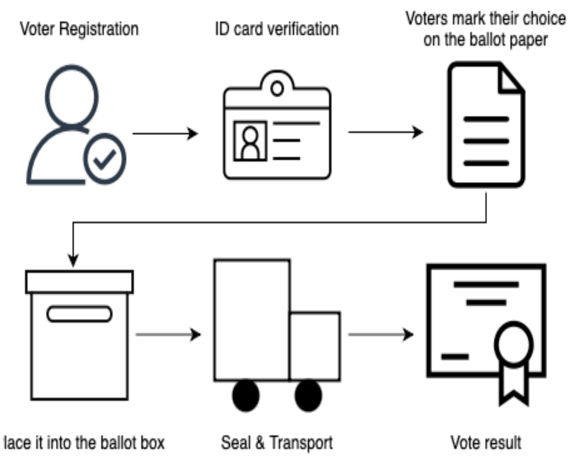

Figure 4. Traditional election process

It is evident that the traditional election process has several significant limitations, including voter data management, identity verification, paper-based voting, and manual counting. These stages are susceptible to errors, delays, and a lack of transparency, as well as opportunities for fraud or data manipulation (Berenjestanaki et al., 2023). These constraints diminish public confidence in election results and incur high costs in terms of time and resources, particularly in national elections with many participants.

Consequently, blockchain-based elections are proposed as a novel alternative that can significantly mitigate the issues found in traditional systems. Key elements of blockchain—namely Privacy, Accessibility, Transparency, and Security—enhance the credibility of the electoral process, reduce delays, and strengthen the trust of eligible voters (El Kafhali, 2024; Benabdallah et al., 2022; Sahib & Al-Shamery, 2021).

To clearly illustrate the differences, Figure 5 presents a comparison between the traditional election process and a blockchain-based election system. By displaying the stages from registration and identity verification to voting, counting, and the announcement of results, it concretely demonstrates how blockchain addresses the limitations of the legacy system and why it is considered a technology with the potential to reform modern electoral systems.

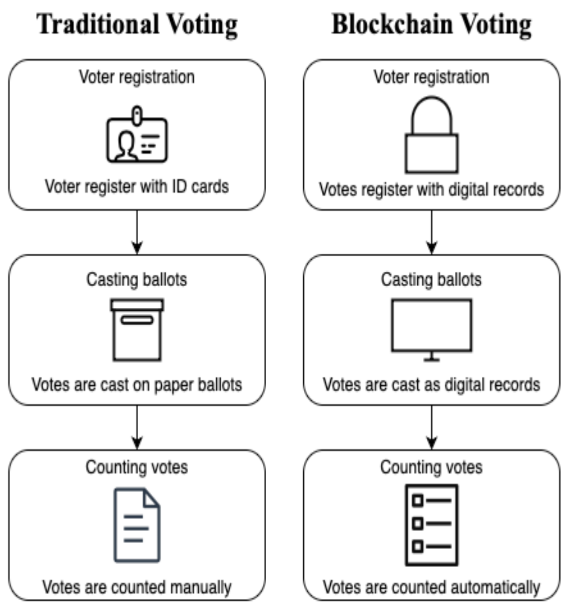

Figure 5. Comparison between traditional and blockchain election processes

Furthermore, to understand the technical differences between traditional election systems and blockchain-based voting, a comparative consideration of five key dimensions consisting of privacy, accessibility, transparency, security, and scalability will clearly highlight the structural advantages of blockchain technology. These specific dimensions serve as the core framework for assessing the potential of election systems in the digital age while reflecting the systemic issues encountered in traditional electoral processes which blockchain systems can concretely address through decentralized and cryptographic mechanisms.

To systematically illustrate this comparison, the researcher has synthesized data derived from relevant academic research and empirical evidence presented in Table 1. This analysis provides a critical evaluation of the comparative levels across the five fundamental dimensions. By juxtaposing the inherent limitations of traditional election systems with the innovative capabilities of blockchain technology, this study highlights how decentralized ledgers can address long-standing vulnerabilities in democratic processes and provide a more resilient framework for modern governance.

Progress and Challenges

The literature review demonstrates a common consensus that blockchain has significant potential to address the limitations of traditional election systems, particularly the issues of vote tampering, result manipulation, corruption, and human error. Numerous studies indicate that core blockchain properties such as transparency, immutability, and security reinforced by cryptographic algorithms like SHA-256 can effectively enhance the credibility of electoral systems (Benabdallah et al., 2022). Most blockchain systems are decentralized, which reduces reliance on central authorities and minimizes the opportunity for interference by any single powerful entity.

Table 1. Comparative Analysis of Electoral System Requirements

Dimensions	Traditional / General E-Voting	Blockchain-based Potential (El Kafhali, 2024)
Privacy	Risk of ballot secrecy being leaked in centralized systems.	Enhanced via ZKPs and identity decoupling to ensure anonymity (Prop. 4, 9).
Accessibility	Limited by physical location or specific proprietary hardware.	Remote access via various devices (Smartphone, Web) at any time (Prop. 3).
Transparency	"Black box" systems; difficult for public auditing.	Open-source nature allows for E2E verifiability and public audit (Prop. 5, 6).
Security	Vulnerable to DoS attacks and data manipulation in central databases.	Immutable ledger prevents double-spending and unauthorized alterations (Prop. 1, 2).
Scalability	Manual counting is slow; some E-voting struggles with high traffic.	Addressed through high-performance frameworks like Hyperledger (Prop. 8).

At the international level, the most frequently mentioned example is the Republic of Estonia, which has successfully implemented an i-Voting system integrated with blockchain (Benabdallah et al., 2022; Çabuk et al., 2018). A key highlight is that the system is designed for transparent auditing and does not permit even system administrators or the government to modify vote data. This serves as a case study that reinforces the potential of blockchain within the context of political trust and modern electoral governance.

Regarding the development of digital voting in Thailand, a significant academic contribution is the B-VoT prototype, which is a Thai blockchain-based voting system designed to enhance data integrity and public trust (Wisessing et al., 2020). This system utilizes Hyperledger Fabric as its core infrastructure to provide a permissioned environment where transactions are immutable and traceable. A critical security feature of B-VoT is its dual-layer authentication, which requires both the national identification number and the verification number located on the back of the ID card. Although the system promotes the convenience of internet-based casting, Wisessing et al. (2020) emphasize that voters should still access the system within controlled environments to ensure proper identity verification. This research serves as a pivotal Thai-based case study demonstrating that integrating blockchain can effectively eliminate human error and prevent the retrospective modification of electoral results.

Comparative Assessment of Voting Methodologies

The evolution of voting systems has led to a diverse range of architectures, each presenting a distinct trade-off between security, privacy, and ease of use. By synthesizing the technical attributes identified in the literature, particularly the work of El Kafhali (2024), we can evaluate the shift from traditional manual processes to complex electronic infrastructures.

Traditional Paper-Based Systems

Traditional methods, where voters mark paper ballots by hand, remain the most common form of voting globally. While they offer a moderate level of privacy through physical isolation in voting booths, they are inherently limited in terms of accessibility and transparency. The reliance on manual labor for counting and the physical logistics of ballot transportation result in low scalability and a high risk of human error or internal fraud. Consequently, as noted by El Kafhali (2024), these systems are often cumbersome and struggle to meet the demands of a rapid, modern electoral cycle.

Legacy Electronic Systems

Early innovations such as Mechanical Lever and Punched Card systems were designed to speed up the tallying process. However, these methods often suffer from low transparency and privacy, as the physical or mechanical recording of votes can be compromised. These legacy systems provide only moderate security and scalability, often failing to provide a verifiable audit trail that can be trusted by the public.

Direct Recording Electronic (DRE) and i-Voting

The introduction of Direct Recording Electronic (DRE) machines significantly improved accessibility, especially for voters with disabilities, and offered high scalability for result generation. However, DRE systems are frequently criticized for their "black box" nature, where the internal processing lacks transparency for public auditing. On the other hand, Internet Voting (i-Voting) provides the highest level of accessibility by allowing participation via personal devices. Yet the security and privacy of i-Voting remain highly variable. El Kafhali (2024) emphasizes that centralized i-Voting infrastructures are vulnerable to large-scale cyber-attacks and lack the immutable auditability required to prevent sophisticated data manipulation.

The Superiority of Blockchain-Based Systems

Considering these historical challenges, blockchain emerges as the "missing puzzle" that harmonizes these conflicting requirements. Unlike centralized electronic systems, blockchain offers a decentralized and open-source architecture that is inherently transparent and auditable. While early models faced scalability hurdles, modern frameworks are evolving to handle large-scale national participants. By ensuring that every vote is "recorded-as-cast" and "tallied-as-recorded" through cryptographic certainty, blockchain addresses the fundamental trust deficit found in traditional and legacy electronic systems.

While blockchain offers a promising solution to the deficits of legacy systems, its practical implementation is not without significant hurdles. One of the significant challenges of applying blockchain to electronic voting systems is scalability, which refers to the system's ability to efficiently handle many voters or transactions, particularly during the peak transaction volumes on election day (El Kafhali, 2024). This challenge stems from the structural limitations of blockchain, such as reliance on consensus mechanisms that require joint processing from multiple computers across the network, limited block sizes for data storage, and increased processing times as transaction volumes rise (El Kafhali, 2024). Numerous studies have identified common issues, including processing delays, network congestion, resource constraints, and operational costs that escalate with the number of users (Benabdallah et al., 2022; El Kafhali, 2024).

To understand the performance differences in transaction volume support among various types of blockchain systems, this research has synthesized technical data and presented it in Table 2 which displays the scalability, consensus mechanisms, and transaction performance of blockchain systems used or proposed for modern electoral systems.

The comparative analysis in Table 2 clearly highlights that while blockchain frameworks—particularly high-performance permissioned systems like Hyperledger Fabric—offer significant advantages over traditional and legacy electronic systems, their successful integration within a specific national context depends on more than just technical specifications. In the case of Thailand, the transition from a manual, paper-based infrastructure to a decentralized ledger involves navigating complex socio-technical challenges, including varying levels of digital literacy and the practicalities of governance.

Therefore, understanding the theoretical superiority of blockchain is only the first step. To determine how these global technical capabilities can be effectively localized and implemented, it is necessary to move beyond the literature and engage directly with domain experts. The following chapter details the qualitative methodology and the five-dimensional framework used to investigate the specific feasibility, risks, and strategic readiness for adopting such transformative technology within the Thai electoral ecosystem.

METHOD

This study employed a qualitative research design, focusing on content analysis as guided by Krippendorff (2004) to gain in-depth insights into the feasibility of blockchain adoption within the Thai electoral system. A qualitative approach was selected to interpret complex phenomena involving technical, legal, and economic dimensions, providing a systematic analytical lens tailored to the national context. The research framework centered on five key aspects: privacy and PDPA compliance, accessibility, transparency, security, and scalability. These dimensions served as the primary criteria for data collection and the subsequent thematic interpretation of the findings.

The target population comprised experts with direct experience in blockchain technology and electoral governance. Following the sampling strategies proposed by Sutheewasinnon and Pasunon (2016), this study utilized purposeful random sampling to ensure the credibility and relevance of the informants. The sample included five key informants: a legal expert (LE) specializing in administrative law and government regulations; two blockchain technology experts (BTE1 and BTE2) with academic and applied expertise in artificial intelligence and databases; an economic expert (EE) with a background in engineering and business management; and a representative from the Election Commission of Thailand (EC) with over ten years of operational experience.

The primary research instrument was a semi-structured interview guide consisting of 20 questions developed from the five-dimension framework. To ensure the quality of the instrument, the questions underwent an Index of Item-Objective Congruence (IOC) assessment by four specialists, following the methodology of Rovinelli and Hambleton (1976). The average IOC score was 1.00, with all items exceeding the acceptable threshold, thereby confirming the validity of the instruments for this study.

Data were collected through in-depth interviews lasting 30–60 minutes per participant. All sessions were audio-recorded and transcribed verbatim, utilizing active listening techniques to ensure accurate interpretation. Ethical standards were strictly maintained; participant identities were anonymized using codes (LE, BTE1, BTE2, EE, EC), and all individuals were informed of their rights prior to the sessions. In line with national guidelines, formal ethical approval was not required as the study posed minimal risk and ensured total confidentiality.

Table 2. Performance comparison of blockchain systems

System	Scalability	Consensus Mechanism	Transaction Performance (TPS)	Privacy	Transparency
Hyperledger Fabric	High	PBFT (Byzantine Fault Tolerance)	20,000+ TPS	High	Moderate
Ethereum (PoW)	Low–Moderate	Proof of Work (PoW)	10–30 TPS	Moderate	High
Traditional System	Low	None	Not specified (Non-digital)	Moderate	Low

Note. Adapted from El Kafhali (2024).

The collected data were analyzed using content analysis (Krippendorff, 2004) to identify and categorize themes across the five framework dimensions. Research quality was ensured through credibility measures, including member checking and verbatim transcription, as well as through confirmability supported by direct quotations. Furthermore, methodological triangulation was applied by comparing interview findings with relevant literature (e.g., Benabdallah et al., 2022) to reinforce analytical rigor and ensure the trustworthiness of the results.

RESULT AND DISCUSSION

The expert interviews provided critical insights into the governance and technical feasibility of blockchain in Thailand. These findings were categorized into five dimensions, reflecting the "Practical Readiness" of the national system.

Privacy and PDPA Compliance: A significant tension exists between voter identification and vote secrecy. While the Legal Expert (LE) noted that electronic systems raise concerns regarding the Personal Data Protection Act (PDPA), the Economic Expert (EE) identified a "KYC Paradox": requiring identity verification on a blockchain seems contradictory to the principle of anonymous voting. To mitigate this, the implementation of Zero-Knowledge Proofs (ZKP) was suggested to verify eligibility without exposing sensitive personal data, which aligns with privacy-preserving models suggested by Berenjestanaki et al. (2024).

Accessibility and Social Impact: Experts recognized blockchain's potential for overseas voters; however, BTE1 emphasized that remote e-voting might compromise election integrity due to voter coercion, as physical booths provide a "safe space" that home-based voting cannot guarantee. This is supported by Mannonov & Myeong (2024), who state that blockchain integration should "support the prevention of fraudulent activities and coercion." Furthermore, the "low ICT skills among the population" identified by Mannonov & Myeong (2024) poses a significant barrier. Without physical support, technology could inadvertently disenfranchise older generations, highlighting the necessity of maintaining physical polling units to bridge this digital divide.

Transparency and the Decentralization Dilemma: A consensus emerged that systems remain vulnerable if controlled by a single group. The EE argued that the system must have no central authority capable of interference, and the government should not develop it alone as a vested stakeholder. This aligns with Khaldun (2025), who emphasizes blockchain's strength in its "decentralized nature where no central authority controls the system," which enhances transparency and allows for independent public auditing.

Security and Future Risks: While blockchain offers immutability through Smart Contracts to prevent double voting, BTE2 warned of future threats from Quantum Computing, which could eventually break current cryptographic standards. This necessitates the adoption of quantum-resistant algorithms to ensure long-term integrity, as suggested by Singh et al. (2023).

Scalability and Economic Viability: Scalability remains the most daunting technical barrier, especially for handling massive transaction volumes in a single day. The EC representative noted that current performance is insufficient for a national election. Consequently, a "Hybrid System" was proposed, where blockchain acts as an auditing layer rather than the primary infrastructure, consistent with Kothari et al. (2025).

Thailand Blockchain Election Readiness Model (TBERM)

To visualize the practical application of block-chain technology within Thailand's diverse social landscape, this study has synthesized its findings into the Thailand Blockchain Election Readiness Model (TBERM) framework. This model is specifically designed to bridge the digital divide and address concerns raised by Mannonov and Myeong (2024) regarding limited digital literacy. The core principle of TBERM is to establish a resilient and inclusive system by integrating a hybrid electoral infrastructure, as illustrated in Figure 6.

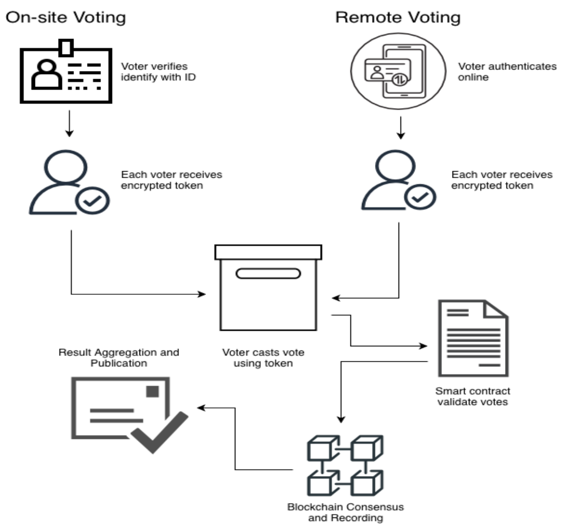

Figure 6. Thailand Blockchain Election Readiness Model (TBERM)

Operational Description of TBERM Model: Figure 6 illustrates the workflow consisting of four primary stages

- Voter Authentication: Supports dual paths: On-site voting at physical units and secure remote online authentication.
- Encrypted Token Issuance: Upon verification, voters receive an encrypted digital token serving as a private key to access the voting platform.
- Vote Casting and Smart Contract Validation: Ballots are cast and automatically validated by Smart Contracts (Chain code) within the Hyperledger Fabric network to ensure all voting criteria are met and prevent double voting.
- Consensus and Decentralized Ledger: Validated votes are permanently recorded onto the Blockchain Ledger via a consortium consensus mechanism, ensuring data immutability.

Operationally, TBERM designates Hyper-ledger Fabric as the core infrastructure for data entry and record-keeping. The researcher selected this permissioned blockchain framework to mitigate scalability limi-tations identified during expert interviews. Hyperledger Fabric offers significantly higher transaction throughput compared to public blockchains and provides robust access control to uphold the principle of anonymous voting through consortium-based node governance.

Furthermore, the risk of voter coercion remains a critical factor for maintaining a hybrid approach. While Mannonov and Myeong (2024) suggest utilizing AI for detection, technology currently cannot fully guarantee physical freedom in unsupervised environments. This aligns with the approach by Wisessing et al. (2020), which emphasizes the necessity of controlled networks at physical polling sites.

Recommendations for Future Research

Building upon the TBERM framework, this study identifies critical limitations for further investigation:

- Addressing Technical Scalability: Although Hyperledger Fabric provides high performance, future studies should focus on fine-tuning and techniques such as Sharding to handle massive nationwide transaction volumes more effectively.
- Developing Anti-Coercion Protocols: Future research should delve into cryptographic mechanisms that guarantee voter freedom, such as "Panic Codes," to bridge the gap where current technology remains limited.

CONCLUSION

In conclusion, this study demonstrates that while blockchain technology offers transformative potential for electoral integrity, Thailand is not yet prepared for full-scale nationwide adoption due to significant technical and digital literacy constraints. To address these systemic barriers, the research proposes the Thailand Blockchain Election Readiness Model (TBERM) as a strategic hybrid roadmap that designates Hyperledger Fabric as the core infrastructure for secure and immutable record-keeping. By integrating this permissioned blockchain framework with traditional physical polling units, TBERM bridges the generational digital divide and provides a haven against voter coercion. Although the model incorporates advanced concepts such as AI-driven surveillance as suggested by Mannonov and Myeong (2024) and automated validation via Smart Contracts, this research acknowledges that a direct, 100 percent solution to physical coercion in unsupervised remote settings, along with nationwide scalability, remains an unresolved socio-technical gap. By synthesizing expert insights into a practical governance structure, TBERM provides a balanced transition path that enhances transparency without disenfranchising vulnerable populations, suggesting that Thailand's evolution toward digital governance must be incremental and committed to developing advanced anti-coercion and high-performance scalability protocols in future democratic innovations.

GRATITUDE

The authors would like to express their sincere gratitude to the experts who provided valuable assistance in validating the research instruments and interview questions, ensuring the quality and rigor of this study. Special thanks are also extended to all participants who dedicated their time for the in-depth interviews; their profound insights and specialized knowledge were fundamental to the analysis and the independent development of the proposed model. Additionally, this research was supported by the College of Digital Technology Innovation, Rangsit University, Thailand. The author gratefully acknowledges the academic guidance and valuable support provided throughout the study.

REFERENCE

Benabdallah, A., Audras, L., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. *IEEE Access, 10*, 70746-70759. https://doi.org/10.1109/ACCESS.2022.3187688

Berenjestanaki, M. H., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-based e-voting systems: A technology review. *Electronics, 13*(1), 17. https://doi.org/10.3390/electronics13010017

Çabuk, U. C., Adıgüzel, E., & Karaarslan, E. (2018). A survey on feasibility and suitability of blockchain techniques for e-voting systems. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(3), 124–132. https://doi.org/10.17148/IJARCCE.2018.7324

Choi, S., Kang, J., & Chung, K. S. (2021). Design of Blockchain-Based E-Voting System for Vote Requirements. *Journal of Physics: Conference Series*, *1944*(1), 012002. https://doi.org/10.1088/1742-6596/1944/1/012002

Daramola, O., & Thebus, D. (2020). Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. *Informatics, 7*(2), 16. https://doi.org/10.3390/informatics7020016

Deviani, R. (2023). A blockchain-based verifiable decentralized mechanism for digital voting systems. *Jurnal Informasi Teknologi Ampera, 4*(3), 298–312. https://doi.org/10.51519/jitaper.v4i3.450

Kafhali, S. (2024). Blockchain-based electronic voting system: Significance and requirements. *Mathematical Problems in Engineering, 2024*, 5591147. https://doi.org/10.1155/2024/5591147

Khaldun, I. (2025). Blockchain technology in elections: Exploring potential and implications. *Jurnal Wacana Politik, 10*(1), 24–32. https://doi.org/10.24198/jwp.v10i1.59073

Kothari, S., Koparde, S., Joshi, S., & Joshi, N. (2025). TrustChain: A blockchain-enabled verifiable digital voting solution for election integrity. *Ingénierie des Systèmes d'Information, 30*(3), 637–645. https://doi.org/10.18280/isi.300308

Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2nd ed.). Thousand Oaks, CA: Sage.

Mannonov, K. M. U., & Myeong, S. (2024). Citizens' perception of blockchain-based e-voting systems: Focusing on TAM. *Sustainability, 16*(11), 4387. https://doi.org/10.3390/su16114387

Mukherjee, A., Majumdar, S., Kolya, A. K., & Nandi, S. (2023). A privacy-preserving blockchain-based e-voting system. *arXiv preprint arXiv:2307.08412*. https://doi.org/10.48550/arXiv.2307.08412

Pereira, B. M. B., Torres, J. M., Sobral, P. M., Moreira, R. S., Soares, C. P. A., & Pereira, I. (2023). Blockchain-based electronic voting: A secure and transparent solution. *Cryptography, 7*(2), 27. https://doi.org/10.3390/cryptography7020027

Reddy, C., Sriraj, K., Gangadhar, C., & Swarnalatha, P. (2021). Blockchain-Based Voting System. *International Journal of Advanced Trends in Computer Science and Engineering, 10*(3), 2015–2018. https://doi.org/10.30534/ijatcse/2021/741032021

Rovinelli, R. J., & Hambleton, R. K. (1976, April). *On the use of content specialists in the assessment of criterion-referenced test item validity.* Paper presented at the Annual Meeting of the American Educational Research Association, San Francisco, CA.

Sahib, R. H., & Al-Shamery, E. S. (2021). A review on distributed blockchain technology for e-voting systems. *Journal of Physics: Conference Series, 1804*(1), 012050. https://doi.org/10.1088/1742-6596/1804/1/012050

Singh, A., Ganesh, A., Patil, R. R., Kumar, S., Rani, R., & Pippal, S. K. (2023). Secure voting website using ethereum and smart contracts. *Applied System Innovation, 6*(4), 70. https://doi.org/10.3390/asi6040070

Sutheewasinnon, P., & Pasunon, P. (2016). Sampling strategies for qualitative research. *Parichart Journal, Thaksin University, 29*(2), 32–48.

Wisessing, K., Ekthammabordee, P., Surasak, T., Huang, S. C. H., & Preuksakarn, C. (2020). The prototype of Thai blockchain-based voting system. *International Journal of Advanced Computer Science and Applications*, *11*(5), 78–84. https://doi.org/10.14569/IJACSA.2020.0110510