JPEPFM Journal of Public Economy and Public Financial Management

Kamu Ekonomisi ve Kamu Mali Yönetimi Dergisi, Cilt: 4 | Sayı: 2 | Ekim 2024

Journal of Public Economy and Public Financial Management, Volume: 4 | Issue: 2 | October 2024

ELECTIONS WITH BLOCKCHAIN TECHNOLOGY: CAN ELECTRONIC VOTING PUT AN END TO THE DEBATES IN TÜRKİYE?

Hakan YILDIRIM[1]

Cihan ÜNAL[2]

Recieved (First): *24.10.2024* ***Accepted:*** *26.10.2024*

Citation/©: Yıldırım H., Ünal C., (2024, Elections With Blockchain Technology: Can Electronic Voting Put An End To The Debates In Türkiye?*, Journal of Public Economy and Pubic Financial Management, 4(2), 112- 132*

Abstract

Elections in Turkey have a long-standing tradition, with citizens going to the polls being considered a hallmark of democratic participation. However, issues related to security, transparency and legitimacy have eroded public trust in the electoral process, especially following events such as the use of unstamped ballots in the 2017 Constitutional Referendum and the annulment of the 2019 Istanbul elections. These concerns are not unique to Turkey; similar issues exist globally.

Around the world, digital solutions are being explored to address these problems. For instance, countries like Estonia, Switzerland and South Korea have integrated blockchain technology into their election processes. In countries such as the United States and Canada, blockchain-based projects have been developed to facilitate voting for citizens living abroad. The transparent, secure and decentralized structure offered by blockchain holds great potential in preventing vote manipulation and ensuring the reliability of election processes.

In Turkey, although SECSIS namely Election Information System digitally manages voter registrations and address information, it does not play a direct role in the voting process. It is important to note the distinction between e-elections and e-voting; e-elections encompass the entire process, while e-voting only involves the act of casting votes. The widespread adoption and acceptance of electronic signatures (e-signatures) also took time, with pilot programs addressing many of the concerns. Similarly, blockchain-supported electronic voting systems have not yet been implemented in Turkey, but it is recommended that this technology be integrated, tested and piloted. By strengthening legal frameworks, enhancing cybersecurity measures and increasing public acceptance, it is believed that blockchain technology could contribute to election security and transparency in Turkey.

Keywords: Blockchain-based election technology, E-voting systems, Election security, Digital ballot, Election transparency.

JEL Codes: K**,** H**,** and O**.**

1. INTRODUCTION

Elections in Turkey have a deep-rooted history, with the tradition of voting have extended back many years. Since the Ottoman Empire, citizens' participation in elections has been considered a significant indicator of democratic maturity and participation. However, issues of security, legitimacy and transparency in election processes have long been at the center of debates for many years.

These debates are not unique to Turkey; globally, democratic elections face similar challenges regarding reliability and transparency. At the core of these debates, which arise in different political and societal contexts, lie universal concerns: accurate vote counting, election security and the protection of voter privacy. The deep trust in election processes in Turkey, rooted in its history, is further strengthened by the perception of voting as an essential civic duty.

[1] Dr., Ankara Bilim Üniversitesi, hakanyildirim72@gmail.com, 0000-0002-5959-2691.
[2] (Sorumlu Yazar/ Corresponding Writer) Dr., Hacettepe Üniversitesi, cihan.unal@hacettepe.edu.tr, 0000-0002-5255-4078.

The fundamental principles sought in democratic elections worldwide are fairness, transparency, voter privacy, security and accountability. These principles are critical in ensuring that every stage of an election is reliable and auditable. In various countries, innovative solutions are being implemented in line with these principles.

This system aims to ensure that votes are recorded transparently and securely while preventing manipulation. South Korea is also among the countries testing blockchain-based voting systems. These countries, which use technology to make elections more transparent and secure, are accelerating digitalization efforts to enhance election security.

In Turkey, blockchain technology is being discussed as a potential solution with similar promise. Blockchain, with its decentralized and transparent structure, can ensure votes are recorded without manipulation and that voter privacy is maintained.This technology could contribute to a secure election process by eliminating human errors and fraud allegations in vote counting. However, questions remain about how this technology could be implemented in Turkey and whether it would resolve the current debates.

E-elections and e-voting are separate concepts. E-elections cover all stages of the election, while e-voting focuses solely on the voting process. Several steps have already been taken for e-elections in Turkey. In this process, SECSIS (Election Information System)plays an important role. SECSIS is a system that manages voters' address and registration information and organizes the election process. However, it is not used as a tool in the voting stage itself but contributes more to the technical infrastructure of the election process.

The e-election process in Turkey bears some similarities to the earlier adoption process of e-signature technology. When e-signature first emerged, there was public resistance regarding its security and accuracy. However, over time, the reliability of e-signatures was proven and their use became widespread. Today, this technology has become standard in digital transactions and there is no longer widespread concern about its security. E-elections may face similar initial skepticism, but pilot projects demonstrating the system’s reliability and transparency could help it gain societal acceptance over time.

Digital solutions for e-voting have not yet been implemented in Turkey. In particular, the use of electronic ballots remains a topic of debate, with discussions considering the potential use of blockchain technology. The security, transparency and immutability that blockchain offers in voting processes have the potential to provide robust solutions to the ongoing debates about election security and transparency in Turkey. The integration of SECSIS and blockchain technologies could be a significant step toward making election processes more reliable. When we look at how blockchain technology is used in elections globally, it is clear that Turkey also has the opportunity to make its election processes more reliable and freer from controversy by investing in these new technologies (Vladucu et al., 2023).

This article analyzes the potential role of blockchain technology in Turkey’s election processes and its contribution to election security and transparency. Our study has adhered to the principles of Neutral, Ethical, Transparent and Objective-NETO, considering transparency, security, accountability and impartiality at all stages of election processes.

The methodology of the research includes a literature review, comparative analysis of national and international practices, security and risk assessment and an examination of the legal framework.

In the findings section, it was concluded that Turkey largely has the necessary infrastructure for e-elections but that the technology should first be tested through small-scale pilot projects before being applied on a broader scale. These projects are critical for identifying and resolving potential technical and societal issues.

In the conclusion and recommendations, it is emphasized that blockchain technology could contribute to Turkey's election security, but steps such as legal regulations, strengthening cybersecurity measures and increasing public acceptance are necessary.

2. THEORETICAL FRAMEWORK

In the context of blockchain-based election systems, the underlying theoretical framework focuses on decentralized trust mechanisms and cryptographic security. Blockchain technology operates on a distributed ledger, where data, such as votes, are stored across multiple nodes, ensuring that no single entity controls or can alter the information. This decentralization provides a significant advantage in terms of transparency and security, addressing long-standing concerns in election processes such as vote manipulation and fraud.

The theory of decentralization is pivotal in understanding blockchain's role in elections. Traditional election systems are typically centralized, with a central authority overseeing vote counting and data management. This creates vulnerabilities, such as the risk of internal manipulation, hacking, or loss of data integrity. Blockchain mitigates these risks by distributing control across a network, making it extremely difficult for any one party to alter the results without consensus from the majority.

Additionally, cryptographic hashing is a key theoretical concept in blockchain, where each block of data (in this case, votes) is linked to the previous one, forming an immutable chain. This ensures that once a vote is cast and recorded, it cannot be changed or tampered with without detection. The concept of consensus algorithms, such as Proof of Work or Proof of Stake, also plays a role in validating and securing the data within the blockchain.

In the Turkish context, the application of these theoretical principles through blockchain technology offers a way to address the country's concerns over election transparency and security. The integration of blockchain into Turkey's electoral system could theoretically enhance trust by providing a verifiable, tamper-proof record of votes while protecting voter anonymity. Furthermore, blockchain aligns with democratic principles by increasing public oversight, as any citizen or authorized observer could independently verify the accuracy of the results through the blockchain network.

Thus, the theoretical foundations of blockchain—decentralization, transparency and cryptographic security—form the basis for its potential application in improving election processes in Turkey, as discussed throughout the article.

2.1. Methodology: Analysing Blockchain Integration in Turkey's Electoral System

In this article, a method has been developed to examine the integration of blockchain technology into Turkey's e-election infrastructure and the impact of this integration on election security. The core approach of the study is based on a literature review and the analysis of existing national and international practices. Particularly, the democratic processes in countries with advanced democracies and the fundamental principles regarding election security have been compared with the advantages offered by blockchain technology. Although some of these examples are still in the preparatory phase, relevant academic discussions have been followed and solution proposals have been utilized.

Literature Review on Blockchain in Electoral Systems: The literature review focuses on international studies and real-world examples of blockchain technology applied to election processes. Blockchain has been widely discussed in academic circles as a means of enhancing transparency, security, and voter privacy in election systems (Berenjestanaki et al., 2024; Vladucu et al., 2023). Countries like Estonia, Switzerland, and South Korea are frequently cited for their progressive approaches to blockchain-based voting systems.

Estonia leads with its fully integrated e-voting system, where blockchain is combined with a robust digital identity infrastructure, ensuring secure and anonymous voting (Smith et al., 2020). Since its operationalization in 2005, it has set a global benchmark for digital elections, demonstrating the potential of blockchain to scale effectively for national elections (Vladucu et al., 2023; Desouza & Somvanshi, 2018).

Switzerland and South Korea are in earlier stages, primarily conducting pilot projects focused on citizens living abroad. These pilots aim to test blockchain's capacity for secure and transparent vote recording. Switzerland emphasizes transparency, allowing voters and third-party auditors to verify that votes have been accurately counted while maintaining voter anonymity (Müller et al., 2022; BlockApps, n.d.).

In Turkey, the SECSIS system, currently used for voter registration and election management, has been frequently discussed as a system that could benefit from blockchain integration (Yılmaz & Acar, 2023). Blockchain's immutability, transparency, and cryptographic security offer the potential to resolve ongoing debates about election security in Turkey (Peelam et al., 2024). According to Vladucu et al. (2023), blockchain systems provide an auditable and tamper-proof platform, enhancing the reliability of e-voting processes by addressing key vulnerabilities in traditional systems.

Through these global examples, it becomes clear that blockchain-based voting systems offer innovative solutions to long-standing election challenges, enhancing security, transparency, and voter trust (Cointelegraph, 2020; Jafar et al., 2021).

Comparative analysis summary: The comparative analysis evaluates the e-election practices of Estonia, Switzerland, and South Korea, comparing them to Turkey's current election infrastructure. Estonia stands as the most developed example, with a fully integrated and secure digital voting system. Switzerland and South Korea have used pilot projects to test blockchain-based voting systems, providing valuable insights into improving election security. Turkey, with its SECSIS system, could potentially enhance election security by integrating blockchain, but

like Switzerland and South Korea, it should begin with small-scale pilots to assess feasibility before large-scale implementation.

Pilot projects for blockchain integration anda roadmap: Throughout the study, the necessity of pilot applications to test the integration of blockchain technology into Turkey's election processes has been emphasized. In this context, suggestions have been provided on how to conduct pilot projects involving a small group of voters, not exceeding 1% of the total electorate. The proposed methodology aims to identify potential technical and societal challenges that may arise during the integration of blockchain technology into election processes. Technical challenges may include issues like system security, data integrity, and voter anonymity, while societal challenges could involve public trust in the system, the ability of voters to use the technology, and concerns over the legitimacy of election results. By identifying these challenges early on, it allows for the development of strategic solutions to address any shortcomings, thereby increasing the system's reliability before it is scaled up for widespread use.

Selection of a small, controlled group: The pilot should focus on a limited voter population (under 1% of total voters) to minimize risk while effectively testing the system's functionality.

Technical testing: The pilot should evaluate the blockchain system's ability to ensure the integrity, transparency and security of votes. This includes assessing the immutability of records, protection of voter anonymity and resistance to tampering or cyberattacks.

Public perception and societal acceptance: Alongside technical evaluations, the pilot should address public concerns about privacy, security and the overall reliability of blockchain-based voting. Public awareness campaigns and transparent communication would be essential in building trust.

Collaboration with legal and regulatory bodies: Ensuring that the pilot is compliant with existing legal frameworks and proposing necessary regulatory adjustments for a broader implementation.

The outcomes of these pilots would provide invaluable insights, guiding the future scalability of blockchain-based voting systems in Turkey and mitigating potential risks in a full-scale rollout.

Risk analysis and security review**:** The potential risks associated with the implementation of blockchain-based election systems in Turkey include critical factors such as cybersecurity threats, deficiencies in technical infrastructure, and voter privacy. These factors have been thoroughly examined, and recommendations regarding the security protocols and measures to minimize these risks have been provided. These risks have been analyzed to ensure a secure and reliable blockchain-based election system in Turkey.

Cybersecurity threats: The system must be protected against potential hacking attempts, denial-of-service attacks and other cyber threats. Advanced encryption and decentralized validation mechanisms inherent in blockchain technology can mitigate some of these risks, but constant monitoring and updates to the security infrastructure will be essential.

Technical infrastructure deficiencies: A successful blockchain-based election system requires robust and scalable digital infrastructure. Turkey's existing infrastructure, particularly SECSIS,

will need to be evaluated and potentially upgraded to ensure compatibility with blockchain technology.

Voter privacy: Maintaining voter anonymity while ensuring transparency is a major challenge in blockchain systems. Strong cryptographic protocols need to be implemented to ensure that votes cannot be traced back to individual voters, protecting the secrecy of the ballot.

To address these risks, the study suggests implementing rigorous security protocols, such as:

Multi-layered encryption to safeguard data at every stage, regular penetration testing to identify and fix vulnerabilities, pilot testing to identify and resolve any technical or societal issues before full-scale implementation.

2.2. Historical and Current Election Controversies in Turkey

Turkey's election history, both during the Ottoman Empire and the Republic, has been marked by numerous controversies involving election security, transparency, and voter privacy. From the violence and manipulation of the 1912 Elections, known as the "Elections of the Clubs," to more recent issues like the 2017 Constitutional Referendum and the 2019 Istanbul Mayoral Election, election processes have frequently been subject to public debate and political tension. Over time, issues such as electoral fraud, pressure on voters, irregularities in voter registration, and disputes over ballot validity have consistently surfaced. These controversies highlight the ongoing challenges Turkey faces in ensuring free, fair, and transparent elections, and they emphasize the need for potential technological solutions, like blockchain and e-voting, to address these issues. However, the adoption of such technologies could also introduce new challenges, requiring careful consideration and planning.

1912 Elections – Elections of the Clubs**:** The term "Sopalı Seçimler" (Elections of the Clubs) refers to the general elections held between 1908 and 1912 during the Ottoman Empire. These elections, particularly the 1912 election, were remembered for the widespread use of violence, coercion and manipulation, which is why they are called by this name. The ruling party of the time, the Committee of Union and Progress (İttihat ve Terakki Cemiyeti), applied heavy pressure on the opposition and resorted to force to secure votes. It is known that both the government and the military intervened in the election process.

Pressure and Violence; During the 1912 election campaign, the Committee of Union and Progress (İttihat ve Terakki Cemiyeti)exerted significant pressure on opposition parties. Opposition representatives in various electoral districts were forced either to vote under duress or to withdraw their candidacies. Additionally, the presence of soldiers at polling stations on election day instilled a great deal of fear among the public.

Election Fraud; Widespread fraud and irregularities were prevalent during the election process. It was frequently reported that vote counting was manipulated to favor the Unionists and that the election results were altered.

Reaction of the Opposition; The opposition party, the Freedom and Accord Party (Hürriyet ve İtilafFırkası), argued that the elections were illegitimate. The protests and objections that followed the elections led to increasing unrest in the country, ultimately accelerating the events leading to the 1913 Raid on the Sublime Porte (Bâb-ı Âli Baskını).

The Elections of the Clubs represent a period in the Ottoman Empire when efforts to transition to modern democratic electoral processes were unsuccessful. These elections are remembered in Turkish political history as a historical example of both political violence and election manipulation.

1950 General Elections – Principle of Secret Ballot, Open Counting:The 1950 general elections represented a historic turning point in Turkey's democratization process. For the first time, the principle of "secret ballot, open counting" was adopted in these elections. However, prior to the announcement of the results, which indicated the victory of the Democrat Party, there were discussions about a potential intervention by the ruling government of the time. While this election is regarded as the starting point of democratic election history in Turkey, it also marked a significant moment for the transparency of election processes (Olgun, 2011).

The 1950 general elections were the first in Turkey to be conducted under judicial oversight, with the assurance of judges supervising the process. This election is considered a pivotal moment in Turkey's democratization journey. The application of the "secret ballot, open counting" principle aimed to ensure that elections were more transparent, fair and trustworthy, taking a critical step to prevent political interference. The elections concluded with the Democrat Party coming to power, securing an important place in Turkey’s democratic history.

1982 Constitutional Referendum – Pressure and Voter Privacy:The 1982 constitutional referendum, held in the aftermath of the military coup, faced widespread criticism for undermining the integrity of the election process. During the referendum, the public was forced to vote under the pressure of the post-coup administration. Serious allegations were made about the lack of voter privacy, as a significant portion of the population reported that they cast a "yes" vote under duress. This referendum stands as a key example in the debates surrounding election security and freedom in Turkey (Soysal, 2023).

2009 Local Elections – Voter Lists and Address Registration System Debates: In the 2009 local elections, serious issues emerged regarding voter lists and the Address Registration System. Many voters discovered on election day that their names were missing from the voter lists at their designated polling stations. The deficiencies in the address registration system prevented some voters from casting their ballots, leading to widespread controversy. Opposition parties claimed that the errors in the lists were made deliberately. This incident sparked a long-standing debate about the transparency and accuracy of Turkey's voter registration system (SETA, 2009).

2010 Constitutional Referendum – Debates Regarding Ballot Boxes:In the 2010 constitutional referendum, debates arose once again regarding election security and the supervision of ballot boxes. Opposition parties, in particular, raised concerns about the potential for fraud in ballot security and the counting process, especially in rural areas. This referendum was marked by high political tension, as critical issues such as democratic rights and judicial independence were put to a public vote through the referendum (Çetinkaya, 2011).

2014 Presidential Election – Debates on Electronic Voting:During the 2014 presidential election, significant debates arose, particularly concerning the voting process for Turkish citizens living abroad. Although electronic voting was considered at the time, it was not implemented due to insufficient technical infrastructure and security concerns. Various

allegations of irregularities emerged regarding the voting process abroad. In particular, concerns were raised about the security of votes cast by mail and the transparency of the counting process (Egeliği, 2024).

2017 Constitutional Referendum – Unstamped Ballots:In the 2017 constitutional referendum, voters were asked whether to approve the transition to a "presidential government system." Following the referendum, the Supreme Election Council (Yüksek Seçim Kurulu - YSK) made a decision on election day to accept unstamped ballots as valid. This decision sparked significant controversy regarding the legitimacy of the referendum results. Opposition parties argued that the inclusion of unstamped ballots compromised the security of the election. In defense of its decision, YSK stated that these ballots did not contain any fraud, but the issue remained a topic of public debate for a long time (YSK, 2017).

2019 Istanbul Mayoral Election – Annulment of the Election:The 2019 Istanbul mayoral election became one of the most heavily debated election processes in Turkey. After Ekrem İmamoğlu was initially declared the winner, the ruling AK Party (Justice and Development Party) lodged objections with the YSK, resulting in the annulment and re-run of the election. The YSK annulled the results, citing irregularities in the vote counting process and the composition of polling station committees. This decision sparked major debates regarding the legitimacy of the democratic process and the protection of voter intent. In the repeated election, İmamoğlu once again emerged victorious, but the entire process left a lasting impact on public discourse (YSK, 2019).

Election processes in Turkey, especially during critical periods, have often been subject to controversy. Issues such as election security, voter privacy and the legitimacy of results have resonated both politically and socially. These past debates have brought forward the potential of new technologies, such as electronic voting and blockchain, as solutions to these challenges. However, it remains uncertain whether the implementation of these technologies will also bring new controversies.

2.3. Comparing Election Principles in Turkey and Global Democracies

Democratic election principles share common foundations globally, though their application varies across different political and cultural contexts. Turkey, like other democracies, strives to uphold essential principles such as fairness, transparency, and accessibility within its electoral system. Examining these principles across different democracies offers insight into both shared values and unique approaches. In this section, we explore these core principles, beginning with the foundational concept of fairness.

2.3.1. Fairness

A fair election system guarantees that every individual has an equal right to vote and that each vote carries the same weight. Fairness typically includes elements such as proportional representation and the absence of fraud or manipulation in vote counting. This principle is closely tied to the concept of "one person, one vote," ensuring that all voters, regardless of their background or location, have an equal say in the election outcome.

Proportional representation aims to ensure that political parties or candidates receive a share of seats in proportion to the votes they receive, reflecting the true will of the electorate. Furthermore, a fair system demands transparency and integrity throughout the voting and counting processes, ensuring that results are accurate and unaltered (Goodwin-Gill, 2006).

2.3.2. Transparency

The transparent conduct of elections means ensuring openness and accountability at all stages of the electoral process. Transparency allows election observers to monitor the process, grants the media and public access to the election proceedings, ensures that results can be verified and fosters trust among voters in the integrity of the process. Transparent elections help guarantee that every step—from voter registration and ballot casting to vote counting and result announcement—is open to scrutiny, reducing the likelihood of fraud or manipulation (Elklit & Reynolds, 2002).

2.3.3. Secret Ballot

In elections, voter privacy ensures that individuals' voting choices remain confidential, allowing them to cast their ballots freely without fear of coercion or pressure. Voter privacy also prevents the manipulation of election results and protects voters from post-election intimidation or retaliation. This principle is a fundamental component of democratic systems, as it guarantees that citizens can exercise their voting rights independently and securely (Katz & Sjoberg, 2022)

2.3.4. Accessibility and Participation

Democratic election systems should promote the participation and access of all individuals in the electoral process. This can be evaluated across a broad spectrum, from physical access (ensuring the accessibility of polling stations) to information access (providing equal access to election-related information). Special attention should be given to facilitating the participation of minority groups, individuals with disabilities and those in rural areas, ensuring that they can vote without barriers and that their voices are equally heard (Birch, 2011)

2.3.5. Accountability

One of the primary goals of election systems is to ensure that the leaders elected are accountable to the people. Voters should be able to hold their representatives accountable through elections and have the power to remove them from office if necessary. Accountability encourages elected officials to act in accordance with the will of the people, ensuring that they remain responsive to the needs and concerns of their constituents (Powell, 2000).

2.3.6. Security and Integrity

Election security involves the accurate verification of voters' identities and the counting of votes without fraud. Ensuring election security requires mechanisms to prevent fraud and manipulation of election results. The integrity of election processes is essential for maintaining the legitimacy of the elections, ensuring that the outcomes truly reflect the will of the people (Norris, 2014).

2.3.7. Equal Representation

Election systems should aim to provide the broadest possible range of representation and ensure the equal representation of diverse groups in society (ethnic, religious, gender, etc.). Fair representation and the protection of minorities are fundamental elements of a democratic election system, ensuring that all segments of society have a voice in governance and that their interests are adequately reflected (Council of Europe, 2016).

2.3.8. Predictability and Legal Safeguards

Election systems must be predictable and operate within a clear set of rules. Any legal objections to election results should be reviewed by independent courts, ensuring that election processes are protected by legal safeguards. In a democratic state governed by the rule of law, elections must rest on strong legal foundations, ensuring fairness and legitimacy (Rose, 2004).

2.4. Election Process in Turkey: Current Stages and Blockchain Potential

The current election system in Turkey is equipped with a series of measures to ensure election security. The security of this system is maintained through both technical safeguards and various institutional mechanisms, ensuring the integrity and transparency of the electoral process.

2.4.1. Turkish Election Informatics System -SECSIS

SECSIS is an election management system used to digitally manage and organize election processes in Turkey. Developed by the YSK, SECSIS aims to conduct the voting, counting and announcement of results in a transparent and secure manner. The main functions of SECSIS include;

Voter Registration and Updates: SECSIS is used to prepare voter lists. All citizens' identification information and voter statuses are recorded in the system and these records are regularly updated to ensure accuracy. Ballot and Vote Counting Process: On election day, voting activities are recorded through SECSIS and vote counts are quickly entered into the system. This allows real-time monitoring of election results and offers protection against potential manipulation.

Announcement of Results: Once votes are counted, the results are transmitted to YSK via SECSIS and the official results are publicly announced through the system.

SECSIS is a critical technology used to ensure election security and minimize human error. However, there have been occasional concerns regarding security vulnerabilities or system transparency. While SECSIS helps centralize vote collection and enables fast results, public discussions sometimes arise over whether there are any security gaps within the system. (YSK, 2024)

2.4.2. Election System and Voting Process

In Turkey, processes such as general elections, local elections and referendums are managed by theYSK. The ballots and ballot boxes used in elections directly reflect the will of the people and the voting process follows these key steps;

Voter Registers: Voters are registered in the voter registry based on their residential address. Each voter is required to vote at a designated polling station. Voters are called to the ballot box after identity verification and cast their vote.

Ballot Papers: The ballot papers display party logos, independent candidates and the names of candidates based on the electoral district. These ballots are printed and distributed by the state and each one is checked by the YSK and election officials.

Voting: Voters cast their votes in a private booth, using a stamp to mark their choice and place the ballot in an envelope. Once the voting process is complete, the envelope is deposited into the ballot box.

Ballot Box Security: Representatives from the participating political parties and independent observers may be present at each ballot box. These individuals are responsible for ensuring the security of the ballot box and the fairness of the vote counting process.

Vote Counting: After the polls close, the votes are counted in the presence of election officials and observers. Once the counting is complete, the results are recorded in an official report and submitted to the YSK to be entered into the digital system for final tabulation.

Election Security Measures (In elections in Turkey, security is ensured through the following measures);

Ballot Security: Ballots are designed and printed by the YSK with special security features to prevent fraudulent ballots from entering the system. These features include paper quality, watermarks and other security markers.

Polling Station Committees and Observers: Each polling station is overseen by committees made up of representatives from all political parties and independent observers. These individuals monitor the voting and counting processes to ensure there are no irregularities or violations.

Electronic Vote Recording Systems: After votes are counted and recorded in official reports, the results are electronically transmitted to YSK's central system. YSK collects and announces the data, which is protected against tampering. Since the voting process is manual, the risk of digital manipulation is minimized.

Oversight by Political Parties: To ensure the reliability of election results, political parties are entitled to send observers to monitor the vote counting process. They also have the right to independently verify results. Many political parties may have parallel vote counting systems in place for additional verification.

Voter Lists and Biometric Records: Voter lists are based on Turkey's address registration system and are updated before each election. With the introduction of biometric data and national ID cards in recent years, it has become more difficult to falsify voter identities.

YSK's Role in Election Security: The YSK is responsible for organizing and supervising elections. In cases of complaints or objections, the YSK has the authority to investigate and address issues through legal channels. It conducts both technical and legal oversight to ensure election security.

Turkey's election system is equipped with security mechanisms to fairly reflect the will of the people. Under the supervision of the YSK, elements such as secure ballots, polling station oversight, electronic result transmission and the right of political parties to observe the process help ensure the security of elections. Despite all these measures, discussions and debates around election security continue to persist.

2.5. Global Case Studies: How Countries Are Adopting Blockchain Voting

According to the data in Table 1, notable countries implementing electronic voting systems include Estonia, Switzerland, South Korea, the United States and Canada. These countries have undertaken pilot projects and comprehensive applications of blockchain-based e-voting systems aimed at improving security, transparency and speeding up election processes. For example, Estonia has successfully used its online e-voting system, integrated with a digital identity infrastructure, since 2005. Meanwhile, Switzerland and South Korea have been testing blockchain technology, particularly for citizens living abroad, with the goal of securely and transparently recording votes.

These examples provide important insights into the potential for countries like Turkey to integrate blockchain technology into their electoral systems and the impact this technology could have on voter confidence and election security.

Table 1. Examples of Electronic Voting Worldwide

Country	Starting Year	E-election/E-voting	Explanation
Estonia	2005	Online E-voting	Integrated with a digital identity system, voters can securely cast their votes online. It boasts the world's most advanced e-voting system.
Switzerland	2000	Pilot projects	A blockchain-based e-voting system is being tested for citizens living abroad. The goal is to develop a transparent and reliable system.
South Korea	2018	Pilot projects	They are testing a blockchain-based e-voting system, primarily for use by citizens living abroad.
US	2018	Pilot projects	Blockchain-based e-voting trials are being conducted for overseas military personnel and citizens living abroad (with a pilot project in the state of West Virginia).
Canada	2010	Municipal e-voting	In the province of Ontario, an online voting system has been successfully implemented in local elections in some municipalities.
France	2005	Pilot projects	E-voting trials for citizens living abroad were conducted but were halted due to security concerns and later re-evaluated.
India	2010	Electronic voting machines	In the country, electronic voting machines are used instead of physical ballots, but online voting has not yet been implemented.
Norvey	2011	Pilot projects	Online voting pilot projects were halted due to security concerns.
Letonia	2021	Municipal pilot applications	Blockchain-based e-voting systems have been tested in local elections.
Brazil	2000	Electronic voting machines	In national elections, electronic voting machines are used and votes are recorded digitally.

Source: Vladucu et al., (2023), www.weforum.org, www.idea.int

2.6. Blockchain Technology in Election Systems

Blockchain technology offers revolutionary solutions in many areas due to its ability to provide secure, transparent and decentralized data management in the digital world. One of the most notable use cases of this technology is the idea of using it as a ballot in election systems. In traditional election systems, the physical security of ballots, the reliability of counting processes and transparency pose significant challenges, while blockchain has the potential to effectively address these issues. (Cointelegraph, 2020)

Blockchain technology offers a revolutionary change in election processes by providing new solutions to critical issues such as vote security, transparency, and data integrity. In this context, the use of blockchain in elections has been tested through pioneering applications in various countries around the world. The tests have yielded and observed the following findings:

2.6.1. Voting Process with Blockchain

The integration of blockchain into election processes enables voters to cast their votes securely in a digital environment. When blockchain is used as a ballot in elections, each vote is added to the chain as a digital block and these blocks are linked together in a sequential manner. This ensures that votes are cryptographically secured on a decentralized network. Each vote can be defined as a digital "ballot," which is recorded in a secure and transparent environment, along with the features offered by blockchain. (Cointelegraph, 2020)

2.6.2. Immutability

One of the fundamental features of blockchain is that once data (the ballot) is added, it becomes immutable. When a voter casts their vote, it is added to the chain as a block and cannot be altered in any way afterward. This prevents the manipulation or accidental alteration of votes during the counting process. In traditional systems, physical ballots can be stolen, destroyed, or counted incorrectly, whereas such risks are eliminated in blockchain. Each vote remains secure from the moment it is added to the chain. (Berenjestanaki et al., 2024)

2.6.3. Voting Secrecy and Anonymity

One of the fundamental principles of democratic elections is voting secrecy. In blockchain-based voting systems, there is no link between voters' identities and their votes. Cryptographic techniques ensure voting secrecy by concealing the identity of voters. For instance, methods like "blind signature" can be used to hide the voter's identity while still allowing their vote to be validated. This way, no authority can learn who the voters voted for, enabling them to vote freely without any pressure. (Sallal et al., 2023)

2.6.4. Verifiability and Transparency of Votes

Another significant advantage provided by blockchain is the verifiability of votes. Each ballot is transparently recorded on the blockchain. Throughout the election process, it is possible to trace how all votes are cast and counted, while voter identities remain confidential. This transparency offers a substantial benefit for election observers and independent organizations. Voters can also verify whether their votes have been accurately recorded, thereby increasing trust in the election results. (Sensing & Systems Group, 2023)

2.6.5. Fast and Reliable Vote Counting

In traditional elections, vote counting can take days or even weeks. During this process, human errors, manipulation and delays can occur. With blockchain-based ballots, these issues are largely eliminated. Since votes are recorded in a digital environment and each stage occurs automatically, counting can be done much faster and more accurately. Technologies like smart contracts facilitate automatic counting processes after the voting phase, allowing results to be obtained in a shorter time. (Singh et al., 2023)

2.6.6. Election Security

The security of elections is one of the most crucial elements of any democratic system. In traditional election systems, the physical security of ballots poses a constant risk of fraud and manipulation. However, blockchain technology minimizes these risks. Operating on a distributed network, blockchain eliminates the risk of a centralized server being compromised. Votes are recorded in encrypted blocks, which can only be verified by all nodes participating in the network. This ensures the integrity of the election process and the reliability of the results. (Jafar et al., 2021)

2.6.7. Accessibility and Ease of Participation

Blockchain technology not only offers a secure and transparent election process but also provides ease of access. Voters can cast their votes online securely without having to physically go to the polling station. This is particularly advantageous for individuals with disabilities, those living in rural areas, or voters abroad. This can increase voter turnout and create a more inclusive democratic process. (BlockApps, 2024)

2.6.8. Accountability and Ease of Audit

Blockchain facilitates the auditing of election results and allows for transparent monitoring. Once each ballot is recorded on the blockchain, it becomes subject to audit. This enables independent observers and relevant authorities to track the vote counting process from start to finish and verify the accuracy of the results. In cases where there are challenges to the election results, blockchain records can be used as evidence, thereby increasing trust in the electoral processes. (Tyma et al., 2022)

2.6.9. Applicability for National and Local Elections

Blockchain can be used in all types of voting processes, from national to local elections. Its decentralized structure allows for secure voting to take place simultaneously in different regions. This enhances the scalability of elections and ensures the system operates smoothly even in high-participation elections. (Desouza & Somvanshi, 2018)

2.6.10. Legal and Technical Challenges

Although blockchain technology holds great potential for use as a ballot in elections, there are also some legal and technical challenges. Factors such as the novelty of the technology and the incomplete legal infrastructure are significant obstacles to the implementation of blockchain-based elections. Additionally, the technical infrastructure used to ensure the security of the

blockchain network must be strong and sustainable. To overcome these challenges, detailed pilot projects and comprehensive legal regulations should be established (Johnson, 2019).

When blockchain technology is used as a ballot in elections, it offers significant advantages in terms of security, transparency and verifiability of votes. Its immutable structure, preservation of voter privacy and auditability can open the door to a new era in election processes. However, for this technology to be widely used, it is necessary to develop the technical infrastructure and legal regulations. In the future, conducting secure, fair and transparent elections using blockchain can contribute to building a stronger foundation for democracy (Peelam et al., 2024).

Table 2. Comparison of Traditional Voting and Blockchain-Based Electronic Voting

Election Principle	Traditional Election Systems	Blockchain-Based Systems
Fairness	Each vote is counted equally; no manipulation in counting.	Immutable record of votes through blockchain (auditability).
Transparency	Open to public oversight, election process can be observed.	Transparent public ledger, blockchain ensures traceability of votes.
Secret Ballot	Voter identity and choices are kept confidential.	Cryptographic methods such as blind signatures ensure voter anonymity.
Accountability	Elected officials are responsible for upholding election fairness and transparency.	Smart contracts and decentralized systems hold the process accountable automatically.
Security	Manual oversight, physical ballot security and trusted officials.	Blockchain and cryptographic protocols ensure the security of votes.
Reliability	Election process is monitored and controlled to ensure accuracy.	Automated pre-vote, vote and post-vote phases monitored by blockchain.
Scalability	Adapted through traditional measures (increased voting stations, extended hours).	Blockchain scales by using consensus algorithms and smart contracts.
Verifiability	Manual audits and recounts ensure vote accuracy.	Verifiability is ensured through cryptographic proofs and immutable records.

Source: Cointelegraph (2020), Berenjestanaki et al. (2024), Sallal et al. (2023), Sensing & Systems Group (2023), and Tyma et al. (2022), www.weforum.org, www.idea.int

3. DISCUSSION: TURKEY'S READINESS FOR BLOCKCHAIN E-VOTING

The question of whether Turkey is ready for e-voting and blockchain technology depends on several factors, including election security, technological infrastructure and public trust. While blockchain-based voting systems promise transparency and secure data management, the feasibility of this technology in a country like Turkey, with a large electorate, remains an important topic of discussion.

Technological Infrastructure: Turkey's extensive fiber optic networks and internet infrastructure seem suitable for digitalization steps like e-voting. However, the effective use of blockchain

technology may require a more specific and advanced digital infrastructure. Additionally, voter internet access and digital literacy will be critical factors.

Security and Transparency: While blockchain technology allows for the transparent monitoring and auditing of election results, security vulnerabilities during implementation, such as cyber-attacks are still a concern. Although Turkey's current SECSIS system has faced some criticisms regarding security, the additional layers of security that blockchain technology could bring might enhance trust in the electoral processes.

Legal Framework and Election Law: There is currently no comprehensive regulatory framework in Turkey for e-voting and blockchain-based systems. Therefore, the legal infrastructure must be prepared and broad public support must be generated for a potential transition to a blockchain election.

In Turkey, elections are governed by a robust legal framework, primarily under the Turkish Constitution and Electoral Law No. 298 (Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun). The YSK is an independent constitutional body responsible for overseeing all aspects of elections, ensuring they are free, fair, and transparent.The YSK manages the entire electoral process, including voter registration, ballot preparation, the conduct of voting, and the resolution of electoral disputes.

The Electoral Law No. 298, first enacted in 1961, provides the primary legal basis for elections in Turkey. Over time, it has been amended to address emerging challenges related to election transparency, security, and voter privacy. Notably, Article 101 of this law stipulates the importance of voter confidentiality and the secrecy of ballots, while other provisions set guidelines for auditing and verifying election results to prevent fraud.

While blockchain technology offers potential solutions for enhancing election security and transparency, its implementation would necessitate significant updates to the current legal framework. New regulations would need to define the processes for casting, recording, verifying, and auditing blockchain-based votes within the context of existing election laws. These changes must ensure compliance with voter privacy regulations (Article 67 of the Constitution) and maintain the integrity of the secret ballot as mandated by Electoral Law No. 298. Additionally, the immutability of blockchain-based vote records would need to align with the legal requirements for election audits and recounts.

Blockchain’s compatibility with current election law raises important questions: Can blockchain ensure a secure and transparent voting system without compromising the core principles of electoral fairness, such as voter anonymity and ballot integrity? Before blockchain technology can be officially integrated into the Turkish election system, the existing legal framework must be adapted to provide legal clarity on these issues.

The Role of Election Law in Pilot Projects: As blockchain-based voting systems are tested through pilot projects, their legal validity must be clearly defined. This would require the establishment of pilot-specific legal frameworks that clarify how blockchain votes will be treated within the larger electoral process. For example, Temporary Election Law Amendments could be enacted to authorize the use of blockchain in a limited scope, such as local or overseas elections, while setting out clear rules for dispute resolution, verification, and auditing.

Furthermore, Article 79 of the Turkish Constitution empowers the YSK to oversee and resolve any disputes arising from the electoral process. This provision would play a critical role in adjudicating potential legal disputes arising from blockchain-based elections, ensuring that voters' rights are fully protected under Turkish law.

By ensuring the legal framework adapts to accommodate blockchain's unique features, Turkey can safely pilot and, potentially, integrate blockchain into its electoral system, improving transparency, security, and voter confidence.

To date, discussions have highlighted that the lack of physical ballots for auditing and potential recounts after the election contradicts the principle of secrecy in elections. However, the first thing blockchain does is prevent a connection between the votes cast and the individuals who cast them. Just like traditional voting, votes in this system are recorded in a certified manner. It is unclear who cast which vote. Additionally, all other election principles and more are upheld. Nevertheless, Turkey's transition to e-voting and blockchain technology requires serious planning and preparation.

4. FINDINGS: BLOCKCHAIN'S ROLE IN SECURING TURKEY'S ELECTIONS

Election security and transparency are cornerstones of democratic processes. Past election controversies in Turkey have opened a window of opportunity for blockchain technology to offer solutions to these challenges. In particular, the decentralized and immutable structure of blockchain technology holds great potential for ensuring election security. However, in the process of developing Turkey's e-voting infrastructure, it is crucial to test these technologies through pilot applications, similar to other countries, with small-scale trials targeting no more than 1% of the population.

What is Blockchain Technology and How is it Used in Elections? Blockchain offers a secure and immutable data management system in the digital environment. Each data block is linked to the previous block and these blocks are stored in a chain. This technology ensures that votes in elections cannot be manipulated, can be transparently monitored and preserves voter privacy.

E-Voting Infrastructure in Turkey: Turkey has already made progress in digital election processes through SECSIS. This system plays a crucial role in improving the transparency of election management and vote counting. However, by integrating blockchain technology with SECSIS, Turkey could address ongoing concerns regarding election security, creating a more robust and secure infrastructure for future elections.

Turkey Has an Important Infrastructure for E-Voting: Turkey largely possesses the necessary infrastructure for e-voting due to its extensive internet infrastructure and digitalization efforts. However, this technology must be addressed not only technically but also in terms of social acceptance. Particularly, starting with pilot projects and conducting trials targeting only a small percentage of the population (not exceeding 1%) is critical for increasing trust in the technology. This way, the innovations brought by blockchain technology can gain more acceptance in society and any potential technical issues can be resolved before they affect large-scale elections.

Global E-Voting Applications and Lessons for Turkey: Countries like Estonia, Switzerland and South Korea are pioneers in blockchain-based voting applications. These countries have successfully tested blockchain-based voting processes integrated with digital identity systems.

Turkey should take steps to strengthen its voting system by benefiting from these experiences, which will facilitate a transition to a secure and transparent e-voting system in the long run.

While Turkey largely has the infrastructure necessary for e-voting and blockchain technology, pilot applications must be conducted before full-scale implementation of these systems. This will increase public trust in these new technologies and resolve discussions regarding election security

5. CONCLUSION AND RECOMMENDATIONS FOR BLOCKCHAIN IN TURKISH ELECTIONS

Discussions surrounding election security and transparency in Turkey could be resolved through the integration of blockchain technology into the electoral processes. With its decentralized and immutable structure, blockchain can prevent the manipulation of votes and offer a reliable election process. Additionally, it provides advantages such as protecting voter privacy, speeding up vote counting and ensuring the reliable announcement of election results. Turkey has significant potential for transitioning to blockchain technology with its existing digital election infrastructure like SECSIS. However, various challenges must be addressed and a comprehensive transition process must be planned before the full-scale implementation of this technology.

Factors such as technical infrastructure, digital literacy, internet access and legal regulations play a critical role in the success of blockchain-based voting systems. While Turkey's current infrastructure is suitable for implementing this technology, it is necessary to test the system's reliability through pilot applications and to increase social acceptance. In particular, small-scale trials targeting no more than 1% of the population can help identify and resolve potential technical issues early on. This will increase trust in blockchain technology and ensure long-term reliability in the electoral processes. We can list the recommendations as follows;

Conduct Pilot Applications: The reliability of blockchain-based voting should be tested through pilot applications at both technical and practical levels. Turkey can evaluate the effectiveness of this technology by conducting small-scale blockchain applications in certain electoral districts or among Turkish citizens living abroad. These trials will enhance public trust in blockchain-based voting systems and highlight potential challenges before transitioning to widespread applications.

Establish Legal Regulations: Comprehensive legal regulations are necessary for the implementation of blockchain-based voting systems in Turkey. It is essential to work on adapting election laws to this new technology, ensuring voter security and the protection of vote privacy and establishing the legal validity of election results. Detailed legislation regarding the electoral processes using blockchain technology should be prepared.

Increase Digital Literacy: Improving the level of digital literacy among voters in Turkey is crucial for them to use blockchain-based e-voting systems effectively. Informational campaigns should be organized, training provided and internet access promoted to help voters understand and trust this technology. This education is particularly critical for individuals in rural areas and those with limited access to digital resources.

Strengthen Cybersecurity Measures: Cybersecurity measures should be enhanced for the security of blockchain-based elections. Protecting the blockchain networks used in electoral

processes from external attacks is a critical necessity for the reliability of the system. Therefore, strengthening Turkey's cybersecurity infrastructure and minimizing vulnerabilities in blockchain networks is important. Additionally, the establishment of independent auditing mechanisms during the electoral processes will increase the reliability of the results.

Prepare Society for This Technology: Transitioning to blockchain-based e-voting systems requires societal acceptance. Therefore, comprehensive information campaigns should be organized to help the public understand the advantages of blockchain technology and how it works. Addressing public concerns regarding this new technology will facilitate broader adoption and reinforce trust in the electoral process. The widespread acceptance of e-signature technology in Turkey's electoral processes is similar to the transition to blockchain-based voting systems. Initially, e-signatures were met with skepticism regarding security and accuracy, but over time they proved to be reliable and have become widely used in digital transactions. Today, there is virtually no discussion regarding the security of e-signatures; rather, this technology has become a standard in everyday digitalization.

Similarly, blockchain-based e-voting systems may initially face resistance. However, pilot projects aimed at testing the reliability of these technologies and the positive results obtained over time can enhance public trust in these systems. Just like the e-signature example, the ability of blockchain to ensure security and increase transparency in electoral processes could lead to widespread acceptance in the long run.

Leverage International Experiences: Successful implementations of blockchain-based voting systems exist in countries like Estonia, Switzerland and South Korea. Turkey can strengthen its voting system by benefiting from the experiences of these countries. Lessons learned from election processes that integrate digital identity systems and blockchain can serve as a guide for Turkey's transition to e-voting.

In conclusion, integrating blockchain technology into election processes has the potential to address issues of election security and transparency in Turkey. However, the careful planning and implementation of the steps mentioned above are necessary for the successful application of this technology.

REFERENCES

Adiputra, C. K., Hjort, R., & Sato, H. (2018). 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) (pp. 22–27). IEEE.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. IEEE Access, 10, 70746–70759.

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

Birch, A. H. (2011). Full participation: A comparative study of democracy and political inclusion. United Nations University Press.

BlockApps. (n.d.). The impact of blockchain on voting systems and governance. BlockApps.

Buchstein, H. (2004). Online democracy, is it viable? Is it desirable? Internet voting and normative democratic theory. In Electronic voting and democracy: A comparative analysis (pp. 39–58). Palgrave Macmillan UK.

Cointelegraph. (2020, February 13). India's citizens will vote with blockchain, election commissioner says. Cointelegraph.

Council of Europe. (2016). Living together as equals in culturally diverse democratic societies. Council of Europe.

Çabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). A survey on feasibility and suitability of blockchain techniques for e-voting systems. arXiv, arXiv:2002.07175.

Çetinkaya, A. (2011). The effects of media reflections of public opinion research about 2010 referendum in Turkey on public opinion (Publication No. 28594626) [Doctoral dissertation, Marmara University]. ProQuest Dissertations & Theses Global.

Desouza, K. C., & Somvanshi, K. K. (2018, May 30). How blockchain could improve election transparency. Brookings.

Egeliği, Ö. E. (2024). Yurt dışında yaşayan Türk vatandaşlarının oy hakkı ve temsili [The right to vote of Turkish citizens living abroad and their representation]. TAÜHFD, 6(1), 386–444.

Elklit, J., & Reynolds, A. (2002). The impact of election administration on the legitimacy of emerging democracies: A new comparative politics research agenda. Commonwealth & Comparative Politics, 40(2), 86–119.Goodwin-Gill, G. S. (2006). *Free and fair elections*. Inter-Parliamentary Union.

Fischer, E. A., & Coleman, K. J. (2007). The direct recording electronic voting machine (DRE) controversy: FAQs and misperceptions. Congressional Research Service, Library of Congress.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983–986). IEEE.

Jafar, U., Ab Aziz, M. J., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors, 21(17), 5874.

Johnson, D. (2019). Blockchain-based voting in the US and EU constitutional orders: A digital technology to secure democratic values? European Journal of Risk Regulation, 10(2), 330–358.

Jones, D. W. (2003). The evaluation of voting technology. In Secure electronic voting (pp. 3–16). Springer.

Katz, R., & Sjoberg, F. M. (2022). Why ballot secrecy still matters. Journal of Democracy, 33(3), 62–76.

Krimmer, R., & Volkamer, M. (2005). Bits or paper? Comparing remote electronic voting to postal voting. In Proceedings of the EGOV (Workshops and Posters), Copenhagen, Denmark, 22–26 August 2005 (pp. 225–232). Citeseer.

Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4), 95–99.

Malhotra, M., Kumar, A., Kumar, S., & Yadav, V. (2022). Untangling e-voting platform for secure and enhanced voting using blockchain technology. In Transforming management with AI, big-data, and IoT (pp. 51–72). Springer International Publishing.

Norris, P. (2014). Why electoral integrity matters. Cambridge University Press.

Olgun, K. (2011). Türkiye'de Cumhuriyetin ilanından 1950'ye genel seçim uygulamaları. Atatürk Araştırma Merkezi Dergisi, 27(79),

Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. Information Processing & Management, 58, 102595.

Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). DemocracyGuard: Blockchain-based secure voting framework for digital democracy. Advance.

Powell, G. B. (2000). Elections as instruments of democracy: Majoritarian and proportional visions. Yale University Press.

Rose, R. (2004). The impact of elections: What voters can expect from the next election. Palgrave Macmillan.

Sallal, M., de Fréin, R., & Malik, A. (2023). PVPBC: Privacy and verifiability preserving e-voting based on permissioned blockchain. Future Internet, 15(4), 121.

Sensing, I., & Systems Group, U. (2023). Blockchain-based electronic voting: A secure and transparent solution. Cryptography, 7(2), 27.

SETA. (2009). 29 Mart 2009 yerel seçimler özel raporu: Türkiye İnsan Hakları Vakfı. SETA.

Soysal, M. (2023). 7 Kasım 1982 tarihli anayasa halk oylaması üzerine bir değerlendirme: Plebisit mi, referandum mu? Çağdaş Türkiye Tarihi Araştırmaları Dergisi, 22(45), 977–1005.

Tanwar, S., Gupta, N., Kumar, P., & Hu, Y.-C. (2023). Implementation of blockchain-based e-voting system. Multimedia Tools and Applications, 1–32.

Tyma, B., Dhillon, R., Sivabalan, P., & Wieder, B. (2022). Understanding accountability in blockchain systems. Accounting, Auditing & Accountability Journal, 35(7), 1625–1655.

Vladucu, M.-V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. IEEE Access, 11, 23293–23308.

Yüksek Seçim Kurulu. (2017). 2017 Türkiye anayasa referandumu sonuçları ve mühürsüz oy pusulaları kararı. YSK Resmi Sitesi.

Yüksek Seçim Kurulu. (2019). 2019/4379 sayılı karar: 2019 İstanbul Büyükşehir Belediye Başkanlığı seçiminin iptali. Yüksek Seçim Kurulu.

Yüksek Seçim Kurulu. (2024). SECSIS (Seçim Bilişim Sistemi). Yüksek Seçim Kurulu.