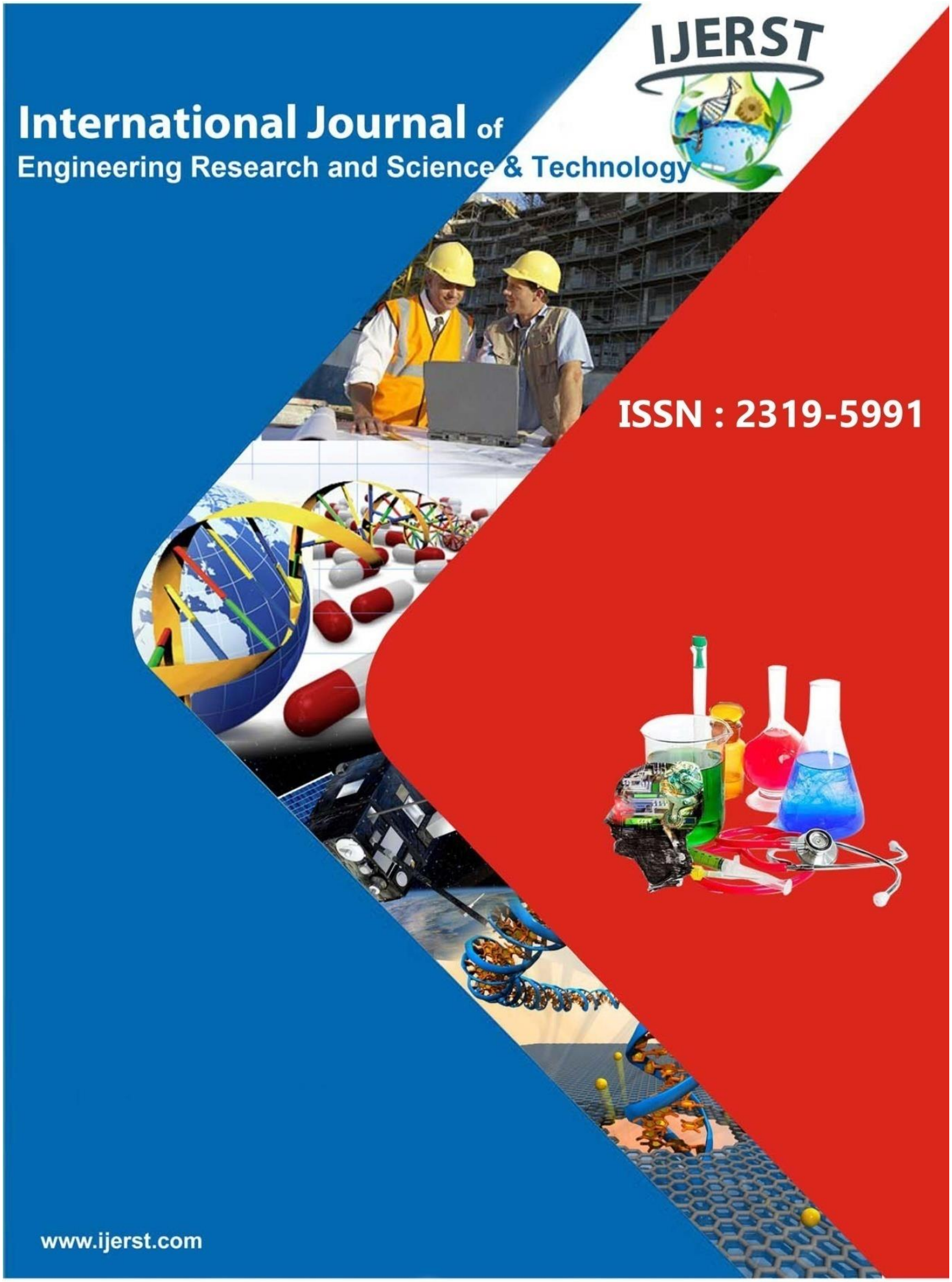

Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issuse.1,Jan 2025

SECURE DIGITAL VOTING SYSTEM

[1]Dr.Joshi Padma,[2]Arepalli Devayani,[3]Kondabathula Rajeshwari Devi,[4]Lakkapatri Akhil,[5]Repaka Dinesh Karthik

[1]Associate Professor,Department Of Computer Science And Engineering,Sreyas Institute Of Engineering And Technology, padmajoshi@sreyas.ac.in.

[2,3,4,5]Students,Department Of Computer Science And Engineering,Sreyas Institute Of Engineering And Technology.

[2]devayaninaidu005@gmail.com, [3]rajia0936@gmail.com, [4]akhillakkapatri9@gmail.com, [5]karthikrepaka777@gmail.com.

ABSTRACT

The advancement of digital technologies has transformed various sectors, including governance and elections. Traditional voting systems, while foundational to democratic processes, are fraught with challenges such as security vulnerabilities, lack of transparency, inefficiencies, and the potential for tampering or fraud. These issues can undermine public trust and raise questions about the integrity of election outcomes. To address these concerns, this project introduces a decentralized voting system leveraging blockchain technology. Blockchain technology provides a decentralized, secure, and transparent platform that eliminates the need for intermediaries and central points of failure. By utilizing tools such as Ganache, MetaMask, Truffle, Solidity, and React, this project creates a tamper-proof, efficient, and user-friendly voting solution. The decentralized nature of blockchain ensures that all transactions, including vote casting and counting, are recorded immutably, thereby enhancing trust in the electoral process. The primary objectives of this project are to provide a secure voting environment, increase transparency in the electoral process, reduce dependence on centralized authorities, and improve accessibility for voters across diverse regions. The proposed solution comprises smart contracts to manage key processes like voter registration, vote casting, and result computation. These smart contracts are deployed on a blockchain network, ensuring transparency and robustness. A user-friendly front-end interface developed using React allows voters to interact with the system seamlessly, while Web3.js

facilitates communication between the front-end and the blockchain.

Keywords: *Digital Voting, Security, Blockchain, Cryptography, Multi-factor Authentication, Voter Anonymity, Real-time Auditing, Election Integrity, Accessibility, Tamper-proof.*

I.INTRODUCTION

A secure digital voting system using blockchain technology offers a revolutionary approach to modernizing elections. By leveraging blockchain's inherent properties of decentralization, immutability, and transparency, this system aims to overcome the challenges faced by traditional voting methods. One of the primary benefits is enhanced security. Each vote is recorded as a transaction on the blockchain, creating an immutable ledger that is virtually impossible to tamper with. This ensures that votes are not altered or deleted once they are cast, providing a high level of confidence in the integrity of the election process . Additionally, blockchain technology enhances transparency in digital voting systems. Since the blockchain is a public ledger, all transactions (in this case, votes) are visible to everyone, ensuring that the entire voting process is transparent and auditable. This openness helps to build trust among voters and stakeholders, as they can verify that their vote has been counted correctly. Furthermore, the decentralized nature of blockchain eliminates the need for a central authority to manage the voting process, reducing the risk of centralized manipulation or fraud. Accessibility is another significant advantage of a blockchain-based voting system. Voters can securely cast their ballots from anywhere in the world using digital devices, making it easier for people who are unable to visit polling stations in person, such as expatriates or individuals with disabilities, to participate in the electoral process. This inclusivity can lead to higher voter turnout and more representative elections. The process begins with voter registration, where individuals' identities are verified and authenticated on the blockchain-based system. Once registered, voters receive cryptographic keys that they use to authenticate themselves before casting their votes. The casting of votes through a secure digital interface is straightforward, and each vote is immediately recorded on the blockchain. The counting of votes is conducted in a transparent manner, with the blockchain providing a verifiable record of all votes cast. In conclusion, a secure digital voting system utilizing blockchain technology presents a promising solution to many of the issues plaguing traditional voting systems. By offering enhanced security, transparency, and accessibility, it has the potential to revolutionize the way elections are conducted, making them more reliable, inclusive, and trustworthy. The primary issue with traditional voting systems is that they are vulnerable to security breaches, lack transparency, and may not be accessible to all eligible voters. To address these challenges, a secure digital voting system utilizing blockchain technology is proposed. The problem statement is as follows: Current voting systems face several significant challenges, including security vulnerabilities, lack of transparency, and limited accessibility. These issues can lead to election fraud, reduced voter confidence, and lower voter turnout. A blockchain-based digital voting system aims to provide a solution by leveraging the decentralized, immutable, and transparent nature of blockchain technology. The system must ensure the following: Security is a top priority in any voting system. Protecting votes from being altered or tampered with requires ensuring the integrity and immutability of the voting records. Each vote should be recorded as a transaction on the blockchain, creating an unchangeable ledger that prevents unauthorized modifications. This guarantees that once votes are cast, they cannot be changed or deleted, thereby securing the election process.Transparency is another crucial aspect of a secure voting system. The blockchain's public ledger feature allows all transactions (votes) to be publicly visible and verifiable. This transparency builds trust among voters and stakeholders by allowing them to audit the voting process and confirm that their votes have been accurately counted. The ability for everyone to verify the integrity of the election process enhances confidence in the results. Accessibility is a significant advantage of a blockchain-based voting system. Enabling eligible voters to cast their ballots securely from any location using digital devices addresses the issue of limited accessibility. This system accommodates individuals who cannot visit physical polling stations, such as expatriates, individuals with disabilities, and those with limited mobility. By increasing voter participation and inclusivity, the system ensures that all eligible voters have the opportunity to contribute to the electoral process. Robust voter authentication mechanisms are essential to ensure that only eligible voters can cast their ballots. Implementing methods such as cryptographic keys, biometric verification, or other secure authentication techniques prevents unauthorized individuals from participating in the voting process. This ensures the legitimacy of each vote and maintains the integrity of the election. Scalability is vital for a digital voting system to accommodate large numbers of voters and transactions without compromising performance or security. The solution should be designed to handle national and local elections efficiently. This ensures that the system can support high voter turnout and maintain its security and transparency features. A user-friendly interface is essential to provide voters with an easy and secure way to cast their ballots.

II.LITERATURE SURVEY

1.Web Service-Based Secure Digital Voting System: A Case Study On Secure Digital Voting System, Jayesh Bhandarkar, This digital solution enables voters to cast their votes via the internet, eliminating the need for traditional paper-based voting. The system is designed to facilitate a secure and efficient voting process, making it more accessible and convenient for voters. It includes features such as voter registration, authentication, vote casting, results tabulation, and robust security measures like mobile OTP verification.

2.Online E-Voting System Using Blockchain, Faizan Sameer Shikalgar, Abhimanyu Digambar Karche, Mansing Vansing Padvi, Raviraj Rangrao Kodag, Prof. S. R. Bhujbal, This paper introduces an Online E-Voting System utilizing Blockchain technology to address challenges associated with traditional voting systems, such as fraud, tampering, and lack of transparency. The proposed system leverages the decentralized and immutable nature of blockchain to establish a secure, transparent, and auditable platform for conducting electronic voting.

3.Decentralized Voting:A Blockchain-Based E- Voting System, L. Schilling, M. H. Raza, S. Kaur, This study presents a decentralized e-voting system using blockchain technology, focusing on voter anonymity, vote integrity, and transparency. The authors discuss the implementation challenges and potential solutions for creating a secure and transparent voting system.

4. A Secure And Transparent Voting System Based On Blockchain Technology, A. Sharma, A. Dhall, This paper proposes a blockchain-based voting system that ensures security and transparency. It describes the system's architecture, including voter registration, authentication, vote casting, and vote counting, and highlights the benefits of using blockchain to enhance the integrity of the voting process.

5.Voting System Using Blockchain Technology: A Review And Future Directions, S. S. Hassan, M. Ali, M. Shahzad, This review paper provides an overview of the current state of blockchain-based voting systems. It examines various use cases, identifies key challenges, and proposes future research directions to improve the security and scalability of blockchain voting platforms.

III.EXISTING SYSTEM

Several Certainly! Here are a few more examples of existing systems and initiatives that utilize blockchain technology for secure digital voting:

1.Voatz: Voatz is a blockchain-based mobile voting platform that has been used in several pilot projects, including elections in West Virginia, Utah County, and Denver. Voatz leverages blockchain to provide a secure and transparent voting process. The platform uses biometric authentication (such as fingerprint or facial recognition) to ensure voter identity, and it encrypts and records each vote on the blockchain. This ensures that votes are tamper- proof and verifiable.

2.Follow My Vote: Follow My Vote is an end-to-end verifiable online voting platform that utilizes blockchain technology to create a secure and transparent voting system. The platform allows voters to cast their ballots online and verify that their votes have been recorded and counted correctly. Follow My Vote's system is designed to prevent election fraud, protect voter privacy, and ensure the integrity of the voting process.

3.Sierra Leone Presidential Election: In 2018, Sierra Leone conducted a blockchain- based pilot for its presidential election. The pilot was implemented by Agora, a blockchain technology company. Agora's platform recorded votes on a blockchain, allowing for a transparent and auditable voting process. The blockchain-based system aimed to reduce the risk of tampering and improve the overall integrity of the election.

4.Moscow's Active Citizen Project: Moscow has implemented a blockchain-based e-voting system for its Active Citizen project, which allows residents to participate in nonpolitical voting on various city initiatives. The blockchain ensures that the voting process is secure, transparent, and tamper-proof. The project has been successful in increasing citizen engagement and trust in the voting process.

5.Estonia's i-Voting System: While not entirely based on blockchain, Estonia's i-Voting system is a pioneer in digital voting. The system uses strong cryptographic techniques to ensure security and integrity. Estonia is exploring the integration of blockchain technology to further enhance the security and transparency of its i-Voting system. The country has been a leader in digital innovation and continues to push the boundaries of secure online voting. These examples demonstrate the potential of blockchain technology to revolutionize the voting process by providing secure, transparent, and accessible platforms for elections. As more governments and organizations explore blockchain-based voting systems, the technology is likely to play an increasingly significant role in future elections.

IV.PROPOSED SYSTEM

The proposed system for a secure digital voting platform using blockchain technology aims to resolve the significant challenges posed by traditional voting methods. These challenges include security vulnerabilities, lack of transparency, and limited accessibility. The proposed system will leverage blockchain's inherent properties of decentralization, immutability, and transparency to ensure a secure, reliable, and inclusive voting process. Voter registration is the first step in the proposed system, where eligible voters register on a blockchain-based voting platform. This process involves verifying the voter's identity using government-issued identification or biometric data. Once verified, voters are issued unique cryptographic keys that they will use for authentication and vote casting, ensuring that only eligible voters can participate in the election. Voter authentication follows, where voters authenticate themselves using their cryptographic keys or biometric data. The system employs multi-factor authentication to add an extra layer of security, ensuring that the voter's identity is legitimate before allowing them to cast their vote. This step is crucial in maintaining the integrity of the voting process by preventing unauthorized access. Vote casting is made simple and secure through a user-friendly digital interface. Voters can access this interface via computers or mobile devices, making it easy for them to cast their ballots from any location. The interface guides voters through the voting process, allowing them to review and confirm their selections before finalizing their votes. This ensures that the voting process is clear and accessible to all eligible voters, regardless of their technological proficiency. Vote recording is handled by the blockchain, which records each vote as a transaction. The blockchain's decentralized and immutable nature ensures that once a vote is recorded, it cannot be altered or tampered with. Each transaction is timestamped and encrypted, providing a verifiable and transparent voting record. This transparency allows stakeholders to audit the voting process and verify the accuracy of the election results.Vote counting is conducted automatically by the blockchain, eliminating the need for a central authority to manage the process. This decentralized approach ensures that the vote counting is transparent and auditable, building trust in the election outcome. Stakeholders can verify the results through the public ledger, further enhancing confidence in the integrity of the voting process. The proposed system includes robust security measures to protect against cyber threats and unauthorized access.

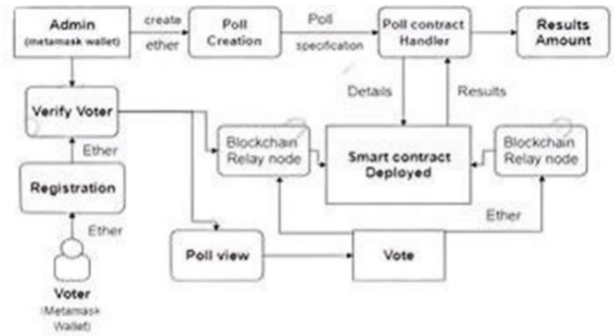

Fig1: Architecture Diagram

V.METHODOLOGY

Implementing a secure digital voting system requires careful planning, development, testing, deployment, and maintenance. A structured implementation methodology is essential to ensure that the system meets both security standards and user requirements throughout its lifecycle. The first step is stakeholder identification and analysis. This phase aims to identify all potential stakeholders and understand their interests, needs, and influence on the project. Activities include conducting stakeholder interviews and surveys to gather insights about their expectations. A stakeholder matrix is created to map out their influence and interest levels, ensuring that key players are properly engaged throughout the process. This foundational step sets the stage for gathering requirements and aligning the project with its intended goals. Next, requirement elicitation is conducted to gather the necessary information from stakeholders. This process uses various techniques, such as workshops and focus group discussions, to foster open communication and collaboration. Additionally, questionnaires and surveys are employed to collect input from a broader range of stakeholders. One-on-one interviews with key individuals further ensure that critical insights are not overlooked. The team may also observe current systems and processes to understand the challenges that the new system needs to address. These activities ensure that the system's design aligns with stakeholder expectations. Once the requirements are gathered, the next step is requirement analysis, which aims to analyze the gathered information for clarity, completeness, and feasibility. This process involves categorizing requirements into functional and non-functional areas, performing feasibility analysis for each, and resolving any conflicts or ambiguities in the data. It is important to prioritize the requirements based on stakeholder input and the overall goals of the project. This analysis ensures that the system's functionality will be feasible and effective in meeting all user and business needs. Following this, the requirements are documented in a clear, concise, and organized manner. A requirements specification document is created to outline all gathered information, including detailed use case diagrams, scenarios, and user stories. The acceptance criteria for each requirement are defined, ensuring that the system meets all expected outcomes. Additionally, process flow diagrams and data models are created to visually represent how the system will operate. This documentation serves as a key reference point for the development team and other stakeholders. Validation and verification are crucial to ensure that the documented requirements accurately reflect stakeholder needs and are feasible to implement. This phase involves reviewing the requirements with stakeholders to confirm that they align with their expectations. Requirement walkthroughs and inspections are conducted to ensure the clarity and completeness of the documentation. Formal approval from stakeholders is obtained before proceeding with the development phase, ensuring all parties are aligned on the project's direction. Lastly, requirement management is an ongoing process throughout the project lifecycle. It is essential to establish a change control process for handling any changes to the requirements as the project progresses. The team tracks and manages requirement changes and assesses their impact on the project. Maintaining a requirements traceability matrix is key to ensuring that all requirements are met and any changes are properly documented and addressed. By following this structured methodology, the secure digital voting system can be developed and deployed in a way that meets both security and usability standards while ensuring that stakeholder needs are effectively addressed throughout the process.

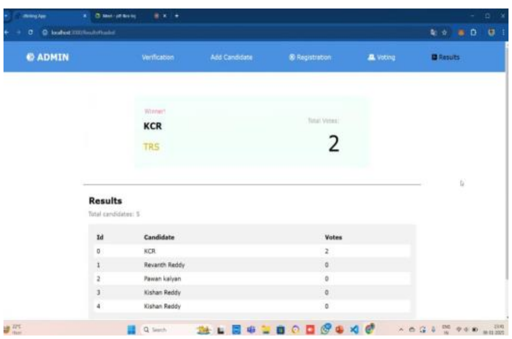

Fig2: Voting Result

VI.CONCLUSION

In conclusion, a secure digital voting system using blockchain technology offers several compelling benefits that make it a promising solution for future elections. By leveraging the decentralized and immutable nature of blockchain, this system ensures a high level of transparency, security, and trust in the voting process. Each vote is recorded as a transaction on the blockchain, making it nearly impossible to alter or tamper with. This provides end- to-end verifiability, ensuring that each vote is counted as intended and can be audited if necessary. Blockchain ensures that every vote is recorded as a unique transaction on a distributed ledger, making it exceedingly difficult for any single entity to manipulate the results. The decentralized nature of blockchain means that no central authority has control over the entire voting process, significantly reducing the risk of fraud and tampering. Each transaction is time-stamped and linked to the previous one, creating a permanent and unalterable record of the voting process. Furthermore, blockchain-based voting systems can enhance voter privacy and security. Through the use of cryptographic techniques, voter identities can be verified without compromising personal information. This ensures that each vote is both anonymous and authenticated, preserving the integrity of the electoral process while protecting voter confidentiality. The end-to-end verifiability offered by blockchain allows voters and election officials to independently verify that votes have been accurately counted, fostering greater trust in the system. Despite the significant advantages, the implementation of blockchain-based voting systems faces several challenges. One of the primary hurdles is the need for extensive technological infrastructure and education. Voters and election officials must be adequately trained and comfortable with using the new system, which may require substantial investment and effort. Additionally, technical challenges such as scalability and network performance must be addressed to ensure that the system can handle large volumes of voters without compromising speed or security.

VII.REFERENCES

1Rockwell, M. (2017) Bitcongress – Process for block voting and law, http://bitcongress.orghttp://bitcongress.org/ last accessed: December 2017 Rosenfeld.

M. (2017).

2.Analysis of hashrate-based double-spending. [Online]. Available: http://arxiv.org/abs//1402.2009 last accessed: December 2017.

3.Nakamoto., S. (2009) Bitcoin: A peer-to-peer electronic cash system, 2009 [Online]. Available: http://bitcoins.info/bitcoin-a-peer-to-peer-electroniccash-system-satoshi-nakamoto. Last accessed: December 2017.

4.Hao, F., Ryan, P. Y. A., and Zielinski, P. (2010) Anonymous voting by two-round public discussion, IET Information Security, vol. 4, no. 2, pp. 62-67, June 2010.

5.Gobel, J., Keeler, H. P., Krzesinski, A.E. and Taylor, P.G. (2015). Bitcoin Blockchain Dynamics: the Selfish-Mine Strategy in the Presence of Propagation Delay, May 2015.

6.Adida, B.; ‘Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335{348.

7.Adida B. and Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting, in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

8.Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). Star-vote: A secure, transparent, auditable, and reliable voting system, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13).

9.Washington, D.C.: USENIX Association, 2013. Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). Bingo voting: Secure and coercion- free voting using a trusted random number generator, in Proceedings of the 1st International Conference on E- voting and

Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

10.Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40 46, May 2008.