

# Voting System: Recent Trends with Blockchain Technology

**Sudin S**

Assistant Professor, Department Mathematics Government engineering College Idukki, Kerala, India

## Abstract

Voting systems play a crucial role in electing representatives in a democratic society. An ideal voting system must be secure, transparent, accessible and ensures the integrity of the electoral process along with improving the participation of all eligible voters by guaranteeing accurate vote counting. This literature survey is a comparative analysis of voting system such as paper ballot, EVM, online voting and emerging voting system on blockchain. It studies the evolution of the various voting system along with addressing the issues related to each system. It explores the strengths and weaknesses of each voting system and technological advancements in each voting system. The study focuses on the need for secure and transparent voting system which utilizes the benefits of blockchain technology. Blockchain technology provides decentralization, accessibility, verifiability, and transparency to address the issues such as trusted third-party involvement, double voting, tampering, privacy, voter authenticity and voter anonymity. This survey analyses the voting systems and provides the scope for future research and the development of a reliable voting system.

**Keywords:** Blockchain, EVM, Paper Ballot, Voting System

## 1. Introduction

Voting systems plays an essential role in the democratic processes. There are always been a concern regarding the reliability of the voting system globally, hence voting systems are always been evolving to enhance reliability and to address the concerns regarding the system. Various voting systems were developed, which includes traditional paper ballots, electronic voting machines (EVMs), online voting and blockchain-based voting systems which is an emerging technology.

Paper ballots are used in the traditional voting system to conduct election. In this system voters have to physically present at the polling station to cast the vote and the votes are counted manually. Since there are trusted third party involvement, there may be chances of malpractices. Also, there is one more issue which can be caused with spread of ink. If the ink spreads, it may lead to smudges or marks and hence the vote gets invalid. EVMs is a solution to the issues with the ink and manual vote counting. These machines have the advantages such as faster results, reduced human errors and automated vote counting. But in this case also the voters have to be physically present at the polling station to cast the vote.

Exponential growth of the internet has led to the growth of the online voting systems. It enables the eligible voters to cast to vote remotely even if they are overseas, hence increases the polling percentage. But security and anonymity must be ensured as internet has potential risk of cyber treats. All these issues can be addressed using the features of the blockchain technology which is secure, transparent and tamper proof as there is no third-party involvement. This literature is an analysis of these voting systems

addressing the advantages as well as the issues.

## 2. Related works

Literature reviews were conducted to study voting system with blockchain. Advancements in technology has a huge impact in traditional voting system. Paper ballot voting has been used for centuries and is a reliable and secure method of voting [1]. It is believed that the first use of paper ballots to conduct an election was in Rome in 139 BCE[1].In paper ballot votes are physically record and can be used as evidence in case of any disputes or recount requests. However, manual vote counting is time-consuming and prone to errors, which can lead to delays in getting the results.

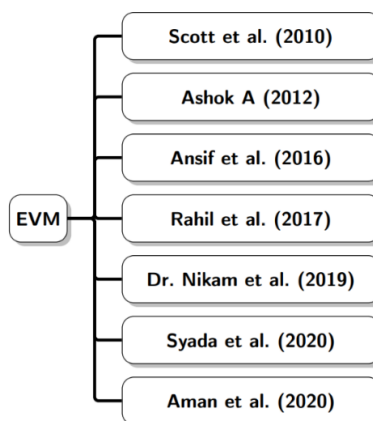
### 2.1. Electronic Voting Machine

Compared to paper ballot voting e-voting and EVMs provide several benefits such as easy to use, speed and accuracy. They provide instant results, in which tedious manual vote counting process can be eliminated. However, there are also some major disadvantages of e-voting and EVMs. One of the biggest concerns is the security of the system, as electronic voting systems can be vulnerable to hacking, tampering or other forms of malicious attacks. In EVMs there are chances of machine tampering, which may lead to incorrect vote counts or incorrect vote casting[2].

The conversion from paper ballot to EVMs is due to the fact that it improves the efficiency, accuracy and speed of the voting process [3]. EVMs has advantages such as reduced human error in counting, quicker result declaration, and difficulty in using inks to cast votes which increases the count of invalid votes. But the security needed to be addressed while considering EVMs for conducting election[2]. EVMs are vulnerable to hardware attack [2]. This can lead to loss of trust in election procedures. Another concern with EVMs is that they are centralized systems, which makes it less transparent and inability for voters to verify if their votes have been accurately counted or not [4].

Biometrically secured EVMs were introduced which enables EVMs to authenticate identity of each voter and prevent double voting [5],[6]. Fingerprints are collected during election and matches with finger prints stored in database. It rejects a voter if the person has already marked the vote. To further improve the accuracy multiple biometric are used [7].It uses both iris recognition and fingerprint for validating a voter. Both iris and fingerprint are considered to a unique biometric character of an individual.

Figure 1. EVM Literature Review



Concerns have been raised regarding the vulnerability of electronic voting machines to malicious programming. If these machines are compromised, hackers could easily manipulate vote counts[8]. Even though paper ballot counting may take longer, people have more trust in traditional process, since machines are susceptible to hacking. Also, machines used in elections may malfunction, which may result in data loss. During manufacturing also, the tampering of electronic voting machines is possible. Fig.1. summarises the various literature on the EVM. Seven works are included in this literature survey to analyse the evolution of EVM with time.

**2.2. Online Voting System without blockchain**

Online voting systems were introduced to conduct election smoothly by reducing the effort of voters taken to participate in the election process and also enables eligible overseas voters to participate in election[9]-[12]. To prevent double voting and to ensure the identity of the voter biometric and SMS based online voting systems where introduced[13], [14]. Two phase authentication mechanism was also introduced to further improve the authentication process [15]. But it failed to protect user data privacy. Since the votes are not encrypted, anonymity is also questionable as there are chances of tracking a vote back to the voter[15].

The SMS-based voting system, guarantees user anonymity by using RSA encryption to encrypt the votes[14]. This means that while the system breaks the link between voter and vote. The biometric based voting system is designed to detect and recognize the face of the voter during election and ensures the identity of the voter along with preventing the voter from casting another vote [13]. The drawback of online voting system includes lack of trust in security of voting process as the system may be vulnerable to hacking or attack such as DOS, spoofing and attacks on DNS [16], [17]. Trusted third party involvement cannot be avoided in this system also hence there may be chances of malpractices[16].

The traditional election system is susceptible to fraud after election as there are involvement of trusted third parties such as Election Commission, Chief Electoral Officer of the State, District Election Officers, Electoral Registration Officers and Returning Officers[18]. Centralized databases, to perform crucial tasks such as vote collection, counting, and auditing which is vulnerable to hacking. Humans involved in the process can be vulnerable to bribery. To overcome these issues researches are being conducting to create a voting system that can be implemented on large scale election using blockchain technology which is decentralised.

**Figure 2. Online Voting System without Blockchain Literature Works**

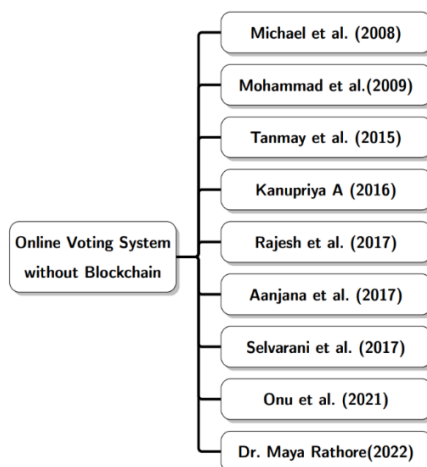


Figure 2 summarises the various literature on the online voting system without blockchain. Nine works are included in this literature survey to analyse the evolution of online voting system without blockchain with time. Table. 1. is a summary of the works related to voting systems such as paper ballot, EVM and online voting systems that does not uses blockchain technology to conduct election.

**Table 1.Literature Review on Voting Systems Without Blockchain**

Type of Voting System	Title	Author	Year
Paper Ballot	A Brief Illustrated History of Voting	Douglas W. Jones	2005
EVM	Security Analysis of India’s Electronic Voting Machines	Scott et al.	2010
	Electronic Voting Machine-A Review	Ashok et al.	2012
	Electronic Voting With Biometric Verification Of-fline And Hybrid EVMS Solution	Ansif et al.	2016
	Biometrically Secured Electronic Voting Machine	Rahil et al.	2017
	A Critical Study of Electronic Voting Machine (EVM) Utilization in Election Procedure	Dr.A.V. Nikam et al.	2019
	From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms	Syada et al.	2020
	Design and Development of Biometric Enabled Advanced Voting System	Aman et al.	2020
Online Voting System without Blockchain	Civitas: Toward a Secure Voting System	Michael et al.	2008
	Modelling and Simulation of a Robust e-Voting System	Mohammad et al.	2009
	Online Voting System	Tanmay et al.	2015
	Issues in implementing of Online Voting System in India	Kanupriya Aggarwal	2016
	Online Voting System	Rajesh et al.	2017
	Confidential E-Voting System Using Face Detection and Recognition	Aanjana et al.	2017
	Secure voting system through SMS and using smart phone application	Selvarani et al.	2017
	Analysis of the Strengths and Weaknesses of Online Voting Systems: the Way Forward	Onu et al.	2021
	A Two-Phase Authentication Mechanism for E-voting in India	Dr. Maya Rathore	2022

**2.3. Online Voting System with blockchain**

The involvement of third parties with malicious intent in the voting system can create problems which is unsolvable in the voting systems mentioned in the above sections. So, we can use blockchain which is a

current trendy technology to address those challenges. A blockchain is a distributed ledger technology that uses cryptography techniques to create an immutable, decentralized database that can store transactions or other data[19]. The data is stored in a decentralized manner, which means that it is not controlled by any single authority or entity, but it is stored in a network of computers.

Blockchain technology was first introduced in 2008 by a person or group of people with pseudonym "Satoshi Nakamoto". They wrote a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" about a digital currency called Bitcoin, which would be decentralized and use blockchain technology to keep it secure [20]. The development of blockchain technology is closely linked to the recession of 2008. In that year, the global financial system was collapsed by many factors, including the housing market bubble and the widespread use in collateralized debt obligations (CDOs).

Trusted third-party banks played a significant role in the financial crisis due to their involvement in the mortgage lending process [21]. Banks and other lenders contributed to the increasing volume of risky loans due to huge competition among lenders. These lenders sold large amounts of loans as mortgage-backed securities (MBS) to investors[21]. The investors including large US banks, as well as foreign banks from Europe and other economies made the risky lending of MBS thinking that they were buying a low-risk assets[21]. Additionally, Banks and investors borrowed more money to expand their lending and buy mortgage-backed securities, but when house prices collapsed, they faced huge losses due to their high levels of borrowing[21]. Also, banks and investors made short-term borrowing, even overnight, to buy assets which is difficult to sell, and hence they dependent on lenders and banks, to provide new loans to repay the existing loan[21].

The first blockchain-based cryptocurrency, Bitcoin, was launched in 2009. It is a decentralized, digital currency that works without the need for a central authority like a bank or government. All transactions made with the currency can be recorded in an unalterable ledger that is maintained by a network of computers around the world. Bitcoin blockchain involves Proof of Work consensus algorithm in which the miner who solves complex mathematical problem to find a key can confirm the transaction and a reward is allotted to the miner. As transactions are encrypted and anonymous, it provides huge security and privacy, hence individuals and organizations began to conduct secure and anonymous transactions without the need for a trusted third party.

Since Bitcoin was created, blockchain technology has been used for more than just cryptocurrency. It can be used in various fields like tracking products in supply chains, financial exchanges, real estate, fair voting system, IoT etc. Blockchain has also led to the creation of other new digital cryptocurrencies like Ethereum. Ethereum uses blockchain to create more advanced computer programs and apps that don't need a central authority to work.

By using blockchain, it is possible to create a more secure, transparent, and decentralized system that can address the concerns related to fraud, tampering, and transparency in the existing voting process[27]. This can ensure the anonymity of the voter along with maintaining the integrity of the voting process. Votes can be encrypted so that manipulations can be prevented. Smart contracts can be used to automate the voting process to reduce the involvement of third parties.

Bosri et al. in 2019 created a voting system using blockchain technology for the storage of votes [32]. The verification process is conducted personally by trusted third parties. As there are involvement of trusted third parties, the possibility of malpractices, such as false voting exists.

In the blockchain based voting systems [22] and [23] authors failed to protect the anonymity as the votes are not encrypted and verifiability was poor as signatures were not implemented in these two systems.

BieVote, A Biometric Identification Enabled Blockchain-Based Voting framework is designed to provide a secure and transparent voting process utilizing Face ID and Fingerprint for authentication [24]. However, since the votes are not encrypted, they are vulnerable to being intercepted or tampered with by third parties, which can compromise the integrity of the election results. Encryption has an important role in breaking the link between the voter and the vote that is casted by the voter.

A double layer encryption model proposed to address result tampering[25]. Votes are encrypted using homomorphic encryption and this encrypted vote is shared among nodes. A major drawback of this system is verification of voter registration is physical which involves trusted third parties. Blockchain can be utilized to enhance security in E-voting applications using IoT devices used in E-polling or counting[26]. This system prevents double voting by using biometric validation. However, if biometric authentication fails some eligible voters may be prevented from casting vote. Also, voter anonymity is not protected as the votes are not encrypted, hence it can lead to third party involvement and vote tampering.

Syada et al. (2022) proposed a system that addresses anonymity, privacy, verifiability and security in a decentralized digital voting system using blockchain technology[27]. However, there are potential issues with voter authentication during the voter registration process, which could result in false voting. A decentralized blockchain-based e-voting system is implemented by Saad et al. 2020, which ensures security for voter's identities [28]. However, one major drawback is that the casted vote is visible and hence anonymity is not ensured. Hence, the vote can be tracked and can lead to vote-buying and can influence the voters to cast false vote.

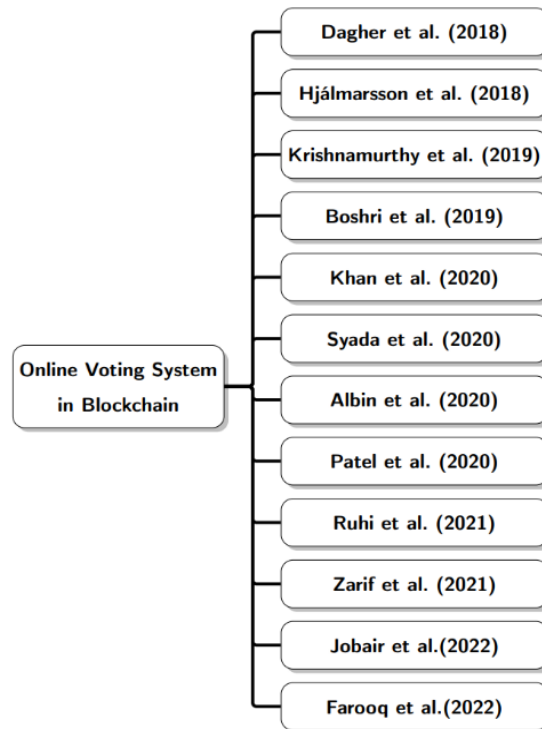
Double voting can be prevented using vote coins [29]. Vote coins are sent to the eligible voters and will get exhausted once a voter cast the vote, thus prevents the voter from casting another vote. But anonymity of the voter may get compromised as the votes are not encrypted instead, they are hashed. The system [30] provide anonymity as the votes are encrypted. Also, blockchain technology ensures transparency by recording and storing votes on a distributed ledger, helps auditing and verification. But there are also drawbacks to consider. One concern is poorly protected method of registration, which could compromise the integrity of the system. Another drawback is weak voter authentication, which could lead to unauthorized individuals participating in the voting process.

Hjálmarsson et al. utilized blockchain technology to conduct a secure election. Encrypted votes are stored in the blockchain, which adds a layer of security to the voting system [31]. But the privacy of the voter data is also needed to be considered. As the voter data is not hashed, there is a concern regarding the privacy of voter information. Hashing makes it computationally difficult to retrieve the original data from the hash.

Figure 3 and Table 2 summarises the various literature on the online voting system in blockchain. Twelve works are included in this literature survey to analyse the evolution of online voting system in blockchain with time.



**Figure 3 Online Voting System with Blockchain Literature Works**



**Table 2 Literature Review on Voting Systems on Blockchain**

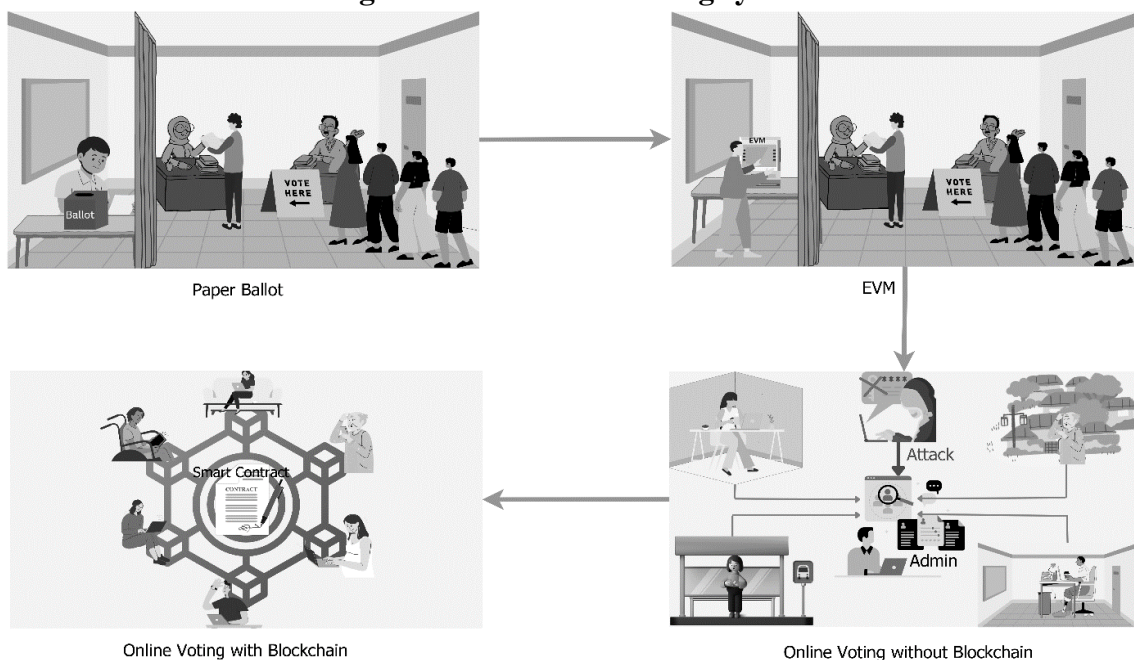
Type of Voting System	Title	Author	Year
Voting System with Blockchain	Broncovote: Secure voting system using ethereum blockchain	Dagher et al.	2018
	Blockchain based e-voting system	Hjalmarsson et al.	2018
	Towards a Privacy-Preserving Voting System Through Blockchain Technologies	Boshri et al.	2019
	An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices	Krishnamurthy et al.	2019
	Blockchain based E-voting System	Albin et al.	2020
	DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system	Syada et al.	2020
	Blockchain technology-based e-voting system	Patel et al.	2020
	Implementation of decentralized blockchain e-voting	Khan et al.	2020
	Blockchain Based E-Voting System: Open Issues and Challenges	Zarif et al.	2021
	A Manipulation Prevention Model for Blockchain-Based E-Voting System	Ruhi et al.	2021
	A Framework to Make Voting System Transparent Using Blockchain Technology	Farooq et al.	2022
	BieVote: A Biometric Identification Enabled Blockchain	Jobair et al.	2022

Based Secure and Transparent Voting Framework		
---	--	--

Fig. 4. illustrates the evolution of voting systems over time. The first voting system uses paper ballot and voters has to tolerate long queue until it is their turn to cast their votes and the votes are counted manually, thus it is prone to errors. The same is applicable for EVM also. But the difference is that, instead of paper ballot, it uses EVM to cast and count the count. In the case of online voting system without blockchain, eligible voters can cast the vote remotely. But there are chances of hacking and vote tampering. In all the above three cases, trusted third party involvement is inevitable. So, it cannot be insured that the system is completely secure.

Voting systems in blockchain can address potentials issues of all other voting system. This system enables to cast votes remotely and securely. It reduces the involvement of trusted third parties and since it is a decentralised, no central authorities are there to control the system. Smart contract can be utilized to automate the process.

**Figure 4 Evolution of voting system**



### 3. Conclusion

From the analysis it is clear that in future the blockchain technology can be utilized to conduct a reliable election which is secure and transparent. The whole election process in the democratic society has to be changed so that the involvement of trusted third party can be avoided and hence election procedure is trustworthy. Individuals and governments are looking forward for the evolution in the system so that every eligible individual can mark their votes easily and securely. Extensive research must be conducted to implement blockchain in voting systems for the elections in future.

### References

1. Douglas W. Jones, "A Brief Illustrated History of Voting", The University of IOWA Dept of Computer Science, 2001, Available at: <https://homepage.cs.uiowa.edu/~jones/voting/pictures/> .
2. Scott Wolchok, Arun Kankipati, Eric Wustrow, Hari K. Prasad, J. Alex Halderman, RopGonggrijp,



- Sai Krishna Sakhamuri, VasavyaYagati. "Security analysis of India's electronic voting machines", In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, 2010, New York, NY, USA, 1–14. <https://doi.org/10.1145/1866307.1866309>.
3. D. Ashok Kumar, T. Ummal Sariba Begum, "Electronic Voting Machine – AReview", Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.
  4. Syada Tasmia Alvi, M. N. Uddin, L. Islam and S. Ahamed, "From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms," 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 2020, pp. 1-6, doi: 10.1109/STI50764.2020.9350399.
  5. Rahil Rezwan, HuzaifaAhmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman, "Biometrically Secured Electronic Voting Machine", 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC) 21 - 23 Dec 2017, Dhaka, Bangladesh.
  6. Ansif Arooj, Mohsin Riaz, "Electronic Voting with Biometric VerificationOffline And Hybrid EVMS Solution", The Sixth International Conference on Innovative Computing Technology(INTECH 2016).
  7. Aman Jatain, Yojna Arora, Jitendra Prasad, Sachin Yadav, Konark Shivam, "Design and Development of Biometric Enabled Advanced Voting System", International Journal of Innovative Research in Computer Science & Technology (IJRCST) ISSN: 2347-5552, Volume-8, Issue-3, May 2020.
  8. Dr.A.V. Nikam, Dr.P.C. Shetiye, Dr.S.D. Bhoite, "A Critical Study of Electronic Voting Machine (EVM) Utilization in Election Procedure", International Journal of Trend in Scientific Research and Development (IJTSRD)Conference Issue, March 2019.
  9. Michael R. Clarkson, Andrew C. Myers, Stephen Chong, "Civitas: Toward a Secure Voting System", 2008 IEEE Symposium on Security and Privacy.
  10. Mohammad Malkawi, Mohammed Khasawneh, Omar Al-Jarrah, "Modeling and Simulation of a Robust e-Voting System", Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765.
  11. Rajesh M. Ghadi, Priyanka S. Shelar, "Online Voting System", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 12, Dec-2017.
  12. Tanmay Kadam, "Online Voting System", International Journal of Engineering Trends and Technology (IJETT), V37(5),273-276 July 2016. ISSN:2231-5381,DOI: 10.14445/22315381/IJETT-V37P247.
  13. AanjanaDevi.S, Dr.Palanisamy.V and Anandha Jothi.R, "Confidential E-Voting System Using Face Detection and Recognition", International Journal of Engineering and Techniques - Volume 3 Issue 4, July-Aug 2017.
  14. X. I. Selvarani, M. Shruthi, R. Geethanjali, R. Syamala and S. Pavithra, "Secure voting system through SMS and using smart phone application", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, India, 2017, pp. 1-3, DOI: 10.1109/ICAMMAET.2017.8186724.
  15. Dr. Maya Rathore, "A Two-Phase Authentication Mechanism for E-voting in India", International Journal of Research in Engineering and Science (IJRES)ISSN (Online): 2320-9364, ISSN (Print): 2320-9356 [www.ijres.org](http://www.ijres.org) Volume 10 Issue 4, 2022, PP. 26-31.

16. Onu, Fergus Uche, Ibe, Walter Eyong, Eneji, Samuel Eneji, “Analysis of the Strengths and Weaknesses of Online Voting Systems: the Way Forward”, IOSR Journal of Mobile Computing & Application (IOSR-JMCA) e- ISSN: 2394-0050, P-ISSN: 2394-0042. Volume 8, Issue 4 (Jul. - Aug. 2021), PP 39-43.
17. Kanupriya Aggarwal, “Issues in implementing of Online Voting System in India”, DOI 10.4010/2016.1294, ISSN 2321 3361, 2016 IJESC.
18. Zarif Khudoykulov, Umida Tojiakbarova, Suhrob Bozorov, Dilshoda Qurbonalieva, “Blockchain Based E-Voting System: Open Issues and Challenges”, 2021 International Conference on Information Science and Communications Technologies (ICISCT), 978-1-6654-3258-0/21/, 2021 IEEE, DOI: 10.1109/ICISCT52966.2021.9670245.
19. Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018), “Blockchain Technology Overview”, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, <https://doi.org/10.6028/NIST.IR.8202>.
20. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.
21. Reserve Bank of Australia, “The Global Financial Crisis”, <https://www.rba.gov.au/education/resources/explainers/pdf/the-global-financial-crisis.pdf>.
22. Prof. Anita A. Lahane, Junaid Patel, Talif Pathan and Prathmesh Potdar, “Blockchain technology-based e-voting system”, ITM Web of Conferences 32, 03001 (2020) <https://doi.org/10.1051/itmconf/20203203001>, ICACC-2020.
23. Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian and Amol Kharat, “Blockchain based E-voting System”(July 11, 2020), Available at SSRN: <https://ssrn.com/abstract=3648870> or <http://dx.doi.org/10.2139/ssrn.3648870>.
24. Md Jobair Hossain Faruk, Mazharul Islam, Fazlul Alam, Hossain Shahriar; Akond Rahman, “BieVote: A Biometric Identification Enabled Blockchain Based Secure and Transparent Voting Framework”, 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA).
25. Ruhi Taş and Ömer Özgür Tanrıöver, “A Manipulation Prevention Model for Blockchain-Based E-Voting Systems”, Security and Communication Networks 2021 Article.
26. R. Krishnamurthy, Geetanjali Rathee, Naveen Jaglan, “An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices”, Published online: 10 August 2019, Springer Science+Business Media, LLC, part of Springer Nature 2019.
27. Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, Sajib Ahamed, “DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system”, Journal of King Saud University – Computer and Information Sciences 34 (2022) 6855–6871.
28. Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khaliq and Tarek Husein, “Implementation of decentralized blockchain e-voting”, EAI Endorsed Transactions on smart cities, 4 (10), 6 2020.
29. M. S. Farooq, U. Iftikhar and A. Khelifi, “A Framework to Make Voting System Transparent Using Blockchain Technology”, in IEEE Access, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.
30. Dagher, Gaby G.; Marella, Praneeth Babu; Milojkovic, Matea; and Mohler, Jordan, “BroncoVote: Secure Voting System Using Ethereum’s Blockchain”, ICISSP 2018: Proceedings of the 4th

International Conference on Information Systems Security and Privacy, 2018-January, 96-107.  
<http://dx.doi.org/10.5220/0006609700960107>.

31. F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjalmtýsson, “Blockchain-Based E-Voting System”, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.
32. R. Bosri, A. R. Uzzal, A. A. Omar, A. S. M. T. Hasan and M. Z. A. Bhuiyan, “Towards a Privacy-Preserving Voting System Through Blockchain Technologies”, 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech), Fukuoka, Japan, 2019, pp. 602-608, doi: 10.1109/DASC/PiCom/CBDCCom/CyberSciTech.2019.00116.



Licensed under Creative Commons Attribution-ShareAlike 4.0 International License