iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43083

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

E-Voting using Ethereum Blockchain

[1]Siddharth Singh, [2]Rohit Prasad, [3]Usha Dhankhar, [4]Dr. Seema Malik
[1, 2]Student, [3, 4]Assistant Professor, Department of Electronics and Communication Engineering, HMR Institute of Technology and Management, New Delhi

Abstract: ***The revolutionary concept of blockchain has given a rise to multiple facets of secure, accountable, online services. We witness the rise of E-voting as a critical topic related to online services. Blockchain with smart contracts emerges as a good candidate to use in the development of safer, cheaper, more secure, more transparent, and easier to use e-voting systems. Ethereum and its network are one of the most viable candidates for the implementation of an e-voting system using blockchain, due to their consistency, widespread use, and provision of smart contracts logic. An e-voting system must be secure, as it should prevent duplication of votes while being fully transparent and protecting the privacy of the voters involved. In this work, we have implemented and tested a sample voting web - application as a smart contract for the Ethereum network using the Ethereum wallets and the Solidity language. Eventually, when elections are held, the Ethereum blockchain will store votes and voting results. Users can connect their Ethereum wallet and vote for the candidate they want to, and these transaction requests are processed by the consensus of each Ethereum node. These agreements create a transparent voting environment.***
Keywords: blockchain, Ethereum, smart-contract, e-voting.

I. INTRODUCTION

Electoral integrity is crucial not only for democratic nations but also for state voters' trust and liability. Political voting methods are crucial in this respect. Electronic voting technologies can boost voter participation and confidence and rekindle interest within the electoral system from a government standpoint. Elections have long been a social concern as an efficient means of creating democratic decisions. Because the number of votes cast in reality increases, citizens have become more conscious of the importance of the voting system. The legal system is the method through which judges judge who will represent in political and company governance. Democracy may be a system of voters electing representatives by voting. The efficacy of such a procedure is decided mainly by the extent of religion that folks have within the election process. The creation of legislative institutions to represent the will of the people may be a well-known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the first resource to specify the desire of the citizens by selecting from the alternatives they made. The standard or paper-based polling method served to extend people's confidence within the selection by majority voting. It's helped make the democratic process and also the voting system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of roughly 200, which are either wholly flawed or hybrid. The key voting model has been accustomed to enhancing trust in democratic systems since the start of the electoral system. It's essential to make sure that assurance in voting doesn't diminish.

A recent study revealed that the standard voting process wasn't wholly hygienic, posing several questions, including fairness, equality, and people's will, which weren't adequately quantified and understood within the variety of governments. Engineers across the world have created new voting techniques that provide some anti-corruption protection while still ensuring that the voting process should be correct. Technology introduced the new electronic voting techniques and methods, which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability compared to manual polling. In contrast to the traditional voting method, it enhanced both the efficiency and also the integrity of the method. Electronic voting is widely utilized in various decisions due to its flexibility, simplicity of use, and cheap cost compared to general elections. Despite this, existing electronic voting methods run the danger of over-authority and manipulated details, limiting fundamental fairness, privacy, secrecy, anonymity, and transparency within the voting process.

Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic legal system, which may be a problem for a transparent voting process in and of itself.

On the opposite hand, the electronic voting protocols have one controller that oversees the entire voting process. This system ends up in erroneous selections thanks to the central authority's dishonesty (election commission), which is difficult to rectify using existing methods. The decentralized network could also be used as a contemporary electronic voting technique to avoid the central authority.

Blockchain technology offers a decentralized node for online voting or electronic voting. Recently distributed ledger technologies like blockchain were used to produce electronic voting systems mainly due to their end-to-end verification advantages. Blockchain is an appealing alternative to traditional electronic voting systems with features like decentralization, non-repudiation, and security protection. It is accustomed to holding both boardrooms and public voting. Initially a series of blocks, a blockchain may be a growing list of blocks combined with cryptographic connections. Each block contains a hash, timestamp, and transaction data from the previous block. The blockchain was created to be data-resistant. Voting could be a new phase of blockchain technology; during this area, the researchers try to leverage benefits like transparency, secrecy, and nonrepudiation that are essential for voting applications. With the usage of blockchain for electronic voting applications, efforts like utilizing blockchain technology to secure and rectify elections have recently received much attention.

II. LITERATURE REVIEW

A lot of practices are made to introduce the variations in voting systems where different techniques and methodologies are used. a number of them guarantee confidentiality and security of the system to some extent, still, the voting information and process have to be controlled and managed with advanced systems that may guarantee the safety and privacy of voters and voter information. Most of the standard voting methodologies rely on a centralized architecture. Centralized storage or centralized architecture is inconvenient if the info is esteemed because unauthorized access and attack by any external agent will challenge the system in terms of reliability. Previous models and architectures are used with the assistance of a centralized architecture approach. which will cause ethical and security problems. Collecting the information at a centralized location puts the information in danger. It is controlled unfairly. So, a good framework overcomes this problem of storing information within the distributed format with the assistance of blockchain. Blockchain could be a distributed ledger that stores all processed transactions in chronological order. Traditional databases are maintained by one organization, which organization has complete control of the database, including the power to control the stored data, censor otherwise valid changes to the information, or add data fraudulently. for many use cases, this is often not a controversy since the organization which maintains the database does so for its benefit, and thus has no motive to falsify the database's contents; however, there are other use cases, like an electoral network, where the info is stored is just too sensitive and therefore the motive to govern it's too enticing to permit any single organization to own total control over the database.

Whether or not it may be guaranteed that the responsible organization would never enact a fraudulent change to the database (an assumption which, for several people, is already an excessive amount to ask), there's still the likelihood that an external agent could break in and manipulate the database to their ends. Blockchain technology solves these problems by creating a network of computers (called nodes) which each store a duplicate of the database, and a group of rules (called the consensus protocol) that outline the order within which nodes may move, adding new changes to the database. In this way, all of the nodes agree on the state of the database at any time, and nobody can falsify the info or censor changes. The blockchain further requires that an audit trail of all changes to the database is preserved, allowing anyone to audit that the database is correct. This audit trail consists of the individual changes to the database, which are called transactions. a gaggle of transactions that were all added by one node on its turn is named a block.

Each block contains relevancy to the block which preceded it, which establishes an ordering of the blocks. This is often the origin of the term "blockchain": it's a series of blocks, each containing a link to the previous block and a listing of recent transactions since that previous block. When a brand-new node joins the network, it starts with an empty database, and downloads all of the blocks, applying the transactions within them to the database, to fast-forward this database to the identical state as all the opposite nodes have. In essence, a blockchain establishes the order within which transactions were applied to the database in the order that anyone can verify that the database is accurate by rebuilding it from scratch and verifying that at no point was any improper change made.

The figure below (figure 1) shows the basic representation of how different 'blocks' are established in a decentralized, chain-type connection. In this entire series of blocks, each block holds a link to the previous block.

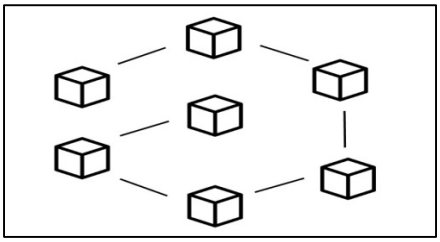


Figure 1

III. IMPLEMENTATION AND DISCUSSION

For our study, we chose to create an e-voting platform on the Ethereum network. As Ethereum supports and nurtures the development of widely-used decentralized apps (or dApps). Ethereum network provides a vast network - size and the ability to enable a smart contract that can run without any downtime, fraud, control, or interference from a third party. Ethereum currently uses a "proof-of-work" consensus which generally means that to add a new block to your existing chain, you need to solve a complex algorithmic problem that might involve a lot of computational power. Solving this problem means you have successfully done some "work" using some computational resources. This process is called mining and if successful, is rewarded with a set amount in ETH. In Ethereum, the blocks are made in real-time and the blocks are validated by the miners. The miners solve a complex algorithmic problem that generates a nonce value which makes a link with the previous block and by this process, all the blocks are connected to form a blockchain. This provides an ideal platform for our e-voting project.

The main concern in E-Voting is to protect the user's identity preserving the transparency and integrity of data while preventing the duplication or manipulation of votes in any way by any external factor. To solve the problem of identity, Ethereum provides a different set of hash values or unique keys to users in the network through which it is almost impossible to identify the individual. The transactions done in the Ethereum network can be viewed by everyone and validated, introducing transparency into the system. To maintain the integrity of the data, the data is not stored in a particular location but is spread across the network which acts as a distributed database making the data immutable and very difficult to manipulate. Through this process, the integrity of the data is maintained. For the process of voting each voter must be provided an Ethereum wallet with its unique key holding a limited amount of ether that will be used to vote for the candidate and the smart contract validates and verifies the voters as well their casted vote.

```
contract Voting {
    int256 public candidate1 = 0;
    int256 public candidate2 = 0;

    mapping(address => bool) public voters;

    function vote1(address voterAddress) public {
        bool checkIfAlreadyVoted = voters[voterAddress];
        if (!checkIfAlreadyVoted) {
            candidate1++;
            voters[voterAddress] = true;
        }
    }

    function vote2(address voterAddress) public {
        bool checkIfAlreadyVoted = voters[voterAddress];
        if (!checkIfAlreadyVoted) {
            candidate2++;
            voters[voterAddress] = true;
        }
    }

    function getResults() public view returns (int256[2] memory) {
        return [candidate1, candidate2];
    }
}
```

Figure 2

Figure 2 shows the smart contract written in Solidity language. We have used two candidates who have participated in the election out of which, only one can win. The voters are validated using a set of conditions and then provided a right to vote for their candidate.

To prevent the duplication of votes, we have used a HashMap data structure. Whenever a user casts a vote, their wallet's unique ID is stored in the HashMap as a key with its value set to true denoting that the user has already cast a vote. If the same user with a similar wallet ID decides to re-cast their vote in the future, they would simply be denied to do so, thus preventing the duplication of votes to some extent. The application is tested on the test network called Metamask. Metamask provides several networks the one used in the project is custom RPC but for final deployment, it should be deployed in the main network. For testing, we created a database of over 50 people ranging across multiple age groups, designations (student, professors, assistant professors), and departments from our college. The purpose of this database was to serve as the voter data for the election of the Head - of - the department for Electronics and Communication Engineering department. In this election, people were provided with their own Ethereum wallets and a limited amount of ether in them for voting purposes. A user would show up at the voting room and connect their Ethereum wallet to the web application. The smart contract would verify the details of the user stored in the database and provide the right to vote only if the user's data satisfied all the parameters shown in the figure below.

```
const { address, candidateNo } = req.body;

    const existingUser = await User.findOne({ address });
    if (!existingUser) {
      throw httpError("User not found");
    }

    if (existingUser.age < 18) {
      throw httpError("User is below 18 yrs of age");
    }

    if (existingUser.department != "ECE") {
      throw httpError("User must belong to ECE Department");
    }

    if (existingUser.designation != "Student") {
      throw httpError("User must be a student");
    }

    res.status(422).send({
      message: "Successfully voted",
    });
```

Figure 3

As it is shown in the figure above (figure 3), the user must be above 18 years of age, should belong to the ECE department, and must be a student. If all these conditions were satisfied, the user was allowed to cast a vote for any candidate.

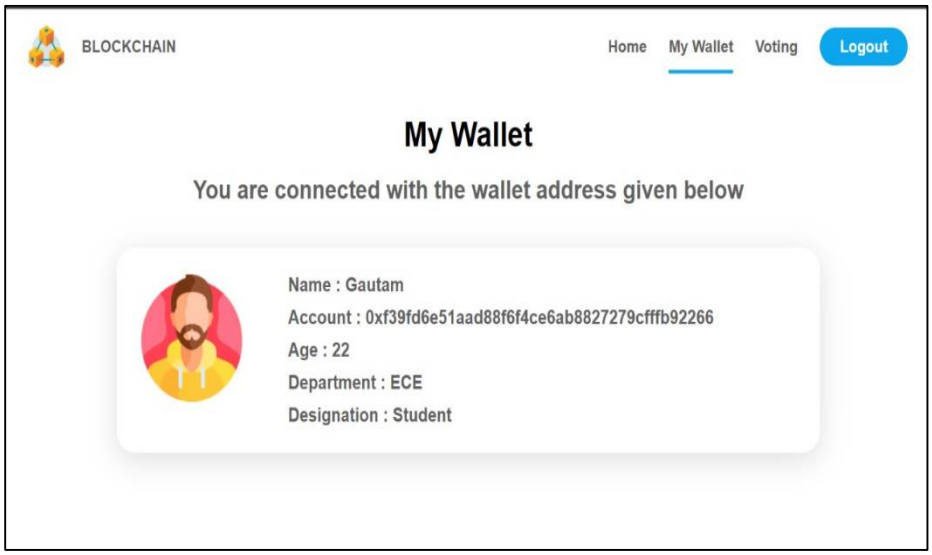


Figure 4

The figure above (figure 4) shows the user that they have successfully connected their Ethereum wallet and registered themselves as a potential voter in the ongoing elections.

To introduce an administrative authority in these elections, we have provided an 'Admin ID' (as shown in the figure above), with its own Ethereum wallet. The admin profile would be able to view the results of the ongoing elections in real-time. This administrator would be the person hosting the elections, the administrator has view-only rights to the election proceedings and in no way can manipulate or tamper with the data involved in the process of elections. At the end of the elections, the administrator can officially declare an end to the voting process and provide the final results to the candidates involved within a few minutes after the end of voting.

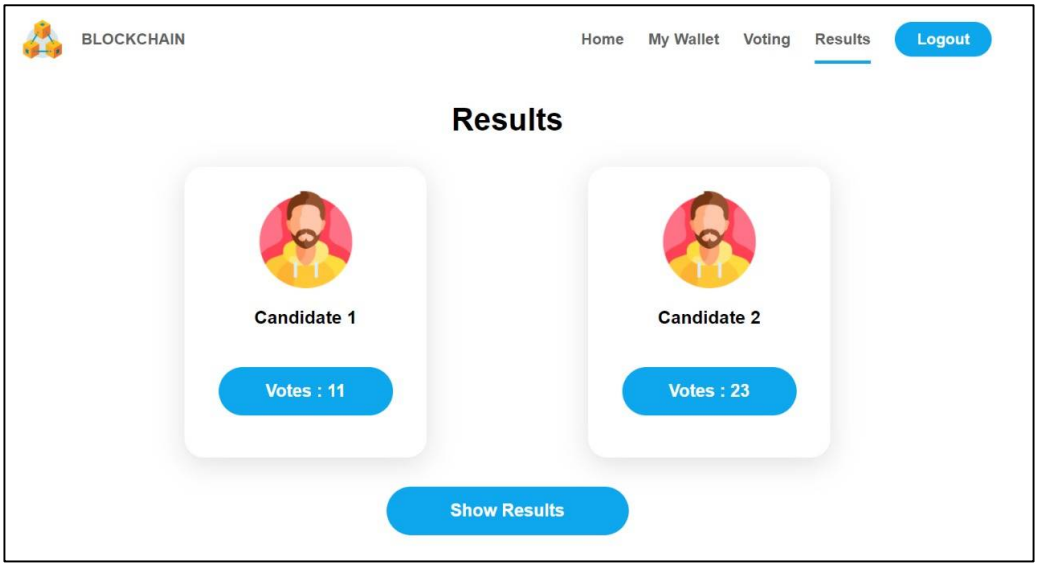


Figure 5

In figure 5, we can see that the 'Results' section is visible along with other options, this 'Results' tab is only available for the administrator and not to a voter.

A. Tools

The prototype application was built and tested on a test network. It was built using the following tools:

Solidity: Solidity is a high-level contract-oriented programming language for executing smart contracts. Solidity is heavily influenced by C++, Python, and JavaScript and is designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed and supports inheritance, libraries, and a user-defined complex type programming language. You can use Solidity to create contracts for purposes like voting, crowdfunding, blind bidding, and multi-signature wallets.

Ethereum: Ethereum is a decentralized platform i.e., a blockchain platform that supports executes smart contracts i.e., applications that work exactly as programmed without any possibility of downtime, censorship, fraud, or third-party interference. The Ethereum Virtual Machine is designed to serve as an execution environment for Ethereum-based smart contracts.

Node.js: Node.js is a server-side platform built on top of Google Chrome's JavaScript engine (V8 engine). Node.js was developed by Ryan Dahl in 2009 and its latest version is v0.10.36. All the APIs in the Node.js library are asynchronous, i.e., non-blocking. Essentially, this means that a Node.js-based server should never expect an API to return data.

MongoDB: MongoDB is a cross-platform, document-oriented database that provides high performance, high availability, and easy scalability. MongoDB works on the concept of collection and document. A collection exists within a single database. Collections do not enforce a schema. Documents within a collection can have different fields.

MetaMask: MetaMask is the trailblazing tool enabling user interactions and experience on Web3. It is currently available as a browser extension and as a mobile app on both Android and iOS devices.

MetaMask allows users to manage their accounts and keys in a variety of ways, including hardware wallets while isolating them from the site context.

IV. CONCLUSION

We tried to shift traditional physical voting methods to a blockchain-based environment. We were able to do all this with the help of the Ethereum network. Which provided us with the necessary tools required to achieve the desired result. We tried to solve the issue of vote tampering, duplicates, and voter validation in our project. At this time, Ethereum and thus the smart contracts, which were one of the most revolutionary breakthroughs since the blockchain itself, helped to shift the limited, narrow perception of blockchain as a cryptocurrency (coin), and turned it into a broader solution-base for a variety of Internet-related problems in the modern world, potentially altering the world's use of blockchain.

In both political and non-political facets of life, E-voting is still a contentious issue. Despite the presence of a few great examples, the majority of them are still in use; more attempts either could not provide the same level of security and privacy as a traditional election or had substantial usability and quantifiability issues. Mostly data protection issues, such as voter privacy, integrity, verification, non-repetition of votes, and investigation transparency, might be addressed (or could be addressed with appropriate modifications).

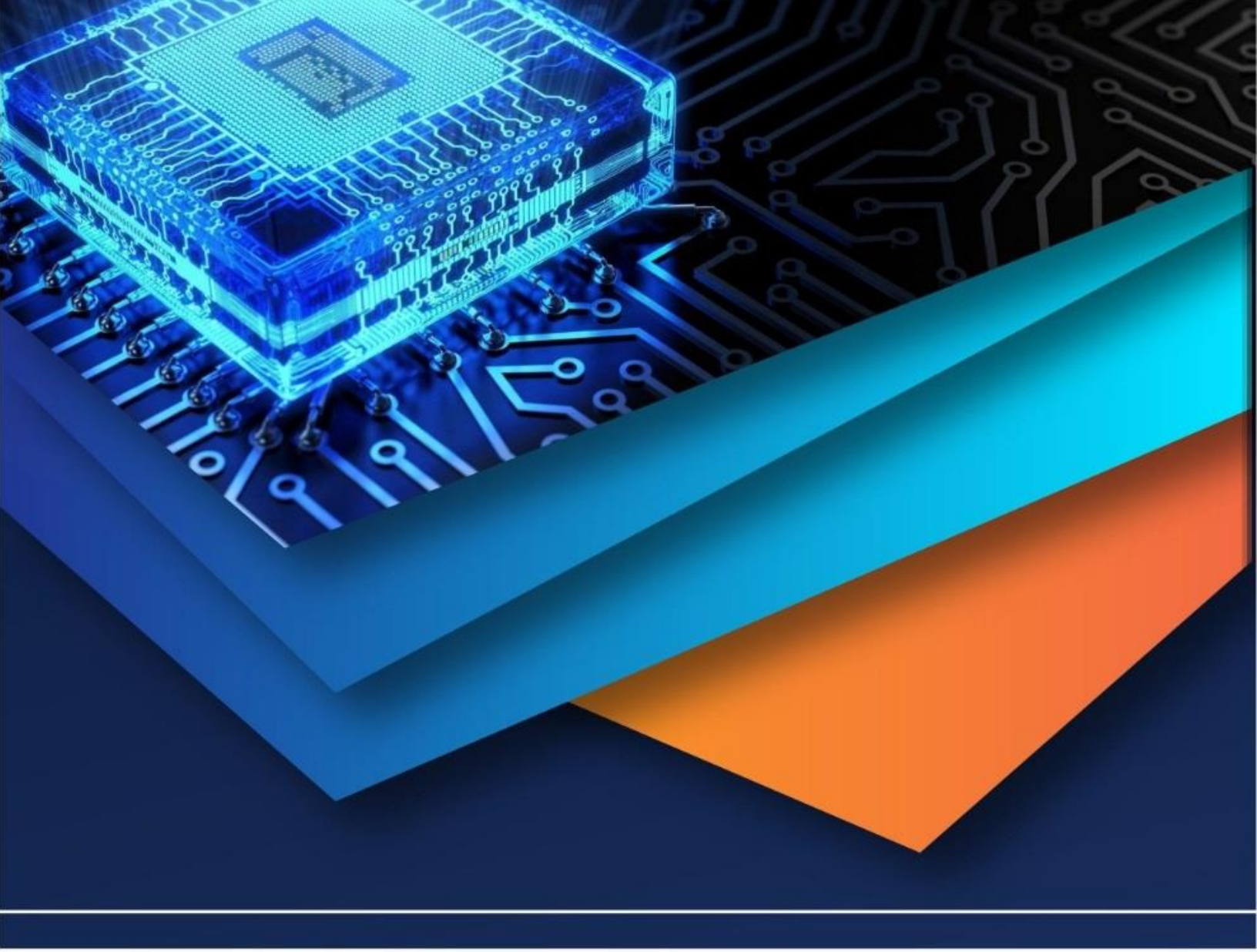
When contemplating the dangers of storing crucial data in a central location, the importance of dispersed systems comes out even more. This could allow authorities to have actual access to voting records on a regular basis, perhaps leading to tampering with data or other malpractices by the authority in charge. Furthermore, in today's linked world, with the concept of the Internet of Things (IoT), various non-computer items are projected to be able to connect to the internet. We continue to work on an itinerant application as a supportive extension of our work to increase usability. As of now, our scope is limited to small-scale polls and elections. A voting event with a voter database in millions comes with its own set of challenges. The scalability of this application depends upon the scalability of the Ethereum network, which is yet to be defined.

V. ACKNOWLEDGEMENT

This study is a part of broader research related to e-voting systems, and we would like to thank all who helped us a lot in completing our project work. Hopefully, it will help in making the voting process fair in the upcoming future.

REFERENCES

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[2] G. Wood, "Ethereum: a secure decentralized generalized transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1- 32, 2014.
[3] C.D. Clack, V.A. Bakshi, and L. Braine, “Smart contract templates: foundations, design landscape and research directions”, Mar 2017, arXiv:1608.00771.
[4] E. Maaten, “Towards remote e-voting: Estonian case”, Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.
[5] U.C. Çabuk, A. Çavdar, and E. Demir, "E-Demokrasi: Yeni Nesil Do÷rudan Demokrasi ve Türkiye’deki Uygulanabilirli÷i", [Online] Available: https://www.researchgate.net/profile/Umut_Cabuk/ publication/308796230_E-Democracy_The_Next_Generation_ Direct_Democracy_and_Applicability_in_Turkey/links/5818a6d408a ee7cdc685b40b/E-Democracy-The-Next-GenerationDirect-Democracy-and-Applicability-in-Turkey.pdf
[6] F. Hao and P.Y.A. Ryan, Real-World Electronic Voting: Design, Analysis and Deployment, CRC Press, pp. 143-170, 2017.
[7] N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe: Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, pp.43-52, 2004. [9] Estonian National Electoral Committee “E-voting System”, 2010. [Online]. Available: https://www.valimised.ee/sites/default/files/ uploads/eng/General_Description_E-Voting_2010.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY