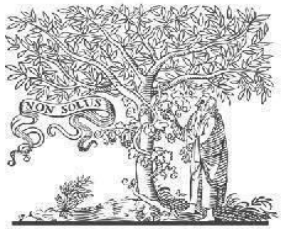
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Dec 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13&issue= Issue12

DOI:10.48047/IJIEMR/V13/ISSUE12/05

Title: " DECENTRALIZED AND SECURE VOTING WITH BLOCKCHAIN"

Volume 13, ISSUE 12, Pages: 43- 53

Paper Authors
Y.Sushma, Dr.B.N.V.MadhuBabu

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DECENTRALIZED AND SECURE VOTING WITH BLOCKCHAIN

Y.Sushma[1], Dr.B.N.V.MadhuBabu[2]

[1]PG Scholar, Department of CSE, TeegalaKrishnaReddyEngineeringCollege (Autonomous Institution),Medbowli, Meerpet, Saroornagar,Hyderabad
[2]Professor, Department of CSE, TeegalaKrishnaReddyEngineeringCollege (Autonomous Institution), Medbowli, Meerpet, Saroornagar, Hyderabad

ABSTRACT

Electronic voting or e-voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. However, there remain challenges to achieve wide spread adoption of such systems especially with respectto improving their resilience against potential faults. Blockchain is a disruptive technology of current era and promises to improve the overall resilience of e voting systems. This paper presents an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for evoting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multichain platform. The paper presents in depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme

Keywords:Cryptography,Evoting technology,Blockchain-enabled e-voting (BEV),Auditable Blockchain Voting System

I. INTRODUCTION

The topic of e-voting systems is still at an early stage of development. We have chosen this domain not only for its recency but also because there are not many solutions that address problems of e- voting. Nowadays, popularity grows also in the development of e-Government. However, such a system is not feasible if basic services for citizens such as elections do not become electronic. "E- voting is one of the key public sectors that can be transformed by blockchain technology". Hand by hand with e-voting come also new challenges, which need to be addressed. One of them is e.g. securing the elections, which needs to be at least as safe as the classic voting systems with ballots. That is why we have decided to create safe elections in which voters do not have to worry about someone abusing the electoral system. In recent years blockchain is often mentioned as an example of secure technology used in an online environment. Our e-voting system uses blockchain to manage all election processes. Its main advantage is that there is no need for confidence in the centralized authority that created the elections. This authority cannot

affect the election results in our system. Another challenge in e-voting is the lack of transparency in the functioning of the system, leading to a lack of confidence in voters. This problem is solved by blockchain in a way of total transparency that allows everyone to see the stored data and processes such as how these 1data are handled. In the field of security, this technology is more suitable in every way than the classic e-voting platform without blockchain.

When consider percentage of voting last few years, it clearly shows vote casting is limited to nearly 75%. That shows 25% voters do not cast their vote. The one of a main purpose of this study is increase the voting percentage though out the country. Here we need to consider all aspects that make voting percentage decrease. People who are outside their city do not wish to come to their city just for voting because of expenses and transportation problems. Some people who works in different cities may not be able attend the voting although they wish to attend. Some people who are on duty during the election they may not get the chance to attend for voting. Peoples with disabilities also may not attend for voting. Disable people cannot access to polling booths easily, but they can easily access online voting system through internet from anywhere. And also by using online voting system voters can vote their own free time within given time period without worrying polling centers. This system will lead to increase the participation to election voting with use of internet. Another main purpose of this study is reduce.

II.RELATED WORK

Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or Smartphone. BEV uses an encrypted key and tamper-proof personal IDs. This article highlights some BEV implementations and the approach's potential benefits and challenges.

Voting Process with Block-chain Technology: Auditable Block-chain Voting System:

There are various methods and approaches to electronic voting all around the world. Each is connected with different benefits and issues. One of the most important and prevalent problems is lack of auditing capabilities and system verification methods. Blockchain technology, which recently gained a lot of attention, can provide a solution to this issue. This paper presents Auditable Blockchain Voting System (ABVS), which describes e-voting processes and components of a supervised internet voting system that is audit and verification capable. ABVS achieves this through utilization of blockchain technology and voter-verified paper audit trail.

Bitcoin: A Peer-to-Peer Electronic Cash System:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to

prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

A Smart Contract for Boardroom Voting with Maximum Voter Privacy:

We present the first implementation of a decentralized and self-tallying internet voting protocol with maximum voter privacy using the Blockchain. The Open Vote Network is suitable for boardroom elections and is written as a smart contract for Ethereum. Unlike previously proposed Blockchain e-voting protocols, this is the first implementation that does not rely on any trusted authority to compute the tally or to protect the voter's privacy. Instead, the Open Vote Network is a selftallying protocol, and each voter is in control of the privacy of their own vote such that it can only be breached by a full collusion involving all other voters. The execution of the protocol is enforced using the consensus mechanism that also secures the Ethereum blockchain. We tested the implementation on Ethereum's official test network to demonstrate its feasibility. Also, we provide a financial and computational breakdown of its execution cost.

Efficient Fully Homomorphic Encryption from (Standard) LWE:

We present a fully homomorphic encryption scheme that is based solely on the (standard) learning with errors (LWE) assumption. Applying known results on LWE, the security of our scheme is based on the worst-case hardness of "short vector problems" on arbitrary lattices. Our construction improves on previous works in two aspects: 1) we show that "somewhat homomorphic" encryption can be based on LWE, using a new re-linearization technique. In contrast, all previous schemes relied on complexity assumptions related to ideals in various rings. 2) We deviate from the "squashing paradigm" used in all previous works. We introduce a new dimension-modulus reduction technique, which shortens the ciphertexts and reduces the decryption complexity of our scheme, without introducing additional assumptions. Our scheme has very short ciphertexts and we therefore use it to construct an asymptotically efficient LWE-based single-server private information retrieval (PIR) protocol. The communication complexity of our protocol (in the public-key model) is k · polylog(k) + log |DB| bits per single-bit query (here, A; is a security parameter).

Definitions and properties of zero knowledge proof systems:

In this paper we investigate some properties of zero-knowledge proofs, a notion introduced by Goldwasser, Micali, and Rackoff. We introduce and classify two definitions of zero-knowledge: auxiliary-input zero-knowledge and blackbox - simulation zero-knowledge

Ethereum: A secure decentralized generalized transaction ledger:

The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not the least being Bitcoin. Each such project can be seen as a simple

application on a decentralized, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalized manner.

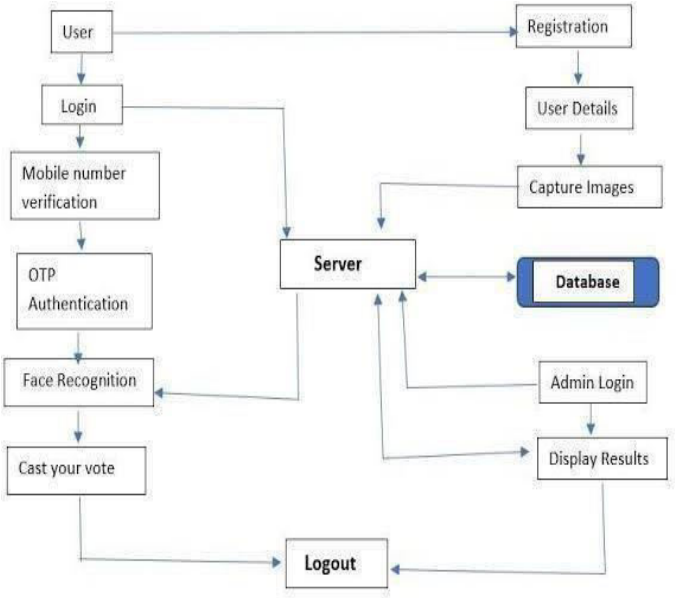


Fig.1. System Architecture

III .IMPLEMENTATION

Python is a general-purpose language. It has wide range of applications from Web development (like: Django and Bottle), scientific and mathematical computing (Orange, SymPy, NumPy) to desktop graphical user Interfaces (Pygame, Panda3D). The syntax of the language is clean and length of the code is relatively short. It's fun to work in Python because it allows you to think about the problem rather than focusing on the syntax.

1.Admin Module: The admin module is a vital component within an electoral system, tasked with managing party and candidate details while overseeing the voting process. Admin users are granted access via predefined credentials, typically a username and password, with 'admin' serving as both username and password for this module. Upon login, administrators are provided with a dashboard facilitating administrative tasks such as adding new parties and candidates. They input relevant information including party names, candidate details, and constituencies. Additionally, administrators can view comprehensive party details, promoting transparency within the electoral process. The module also empowers administrators to monitor vote counts in real-time, enabling them to track voter turnout and detect any irregularities. Through these functionalities, the admin module ensures the integrity and efficiency of the electoral system, contributing to fair and transparent elections.

2.User Module: This user has to sign up with the application by using username as his ID and then upload his face photo which capture from webcam. After registering user can go for login which validate user id and after successful login user can go for cast vote module which execute following functionality

1.First user will be connected to his PC webcam and then image will be capture

2.Using OpenCV application will detect face and then using CNN application will predict user identify and if user identity matched with CNN predicted face then application will display all voting candidate slist.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

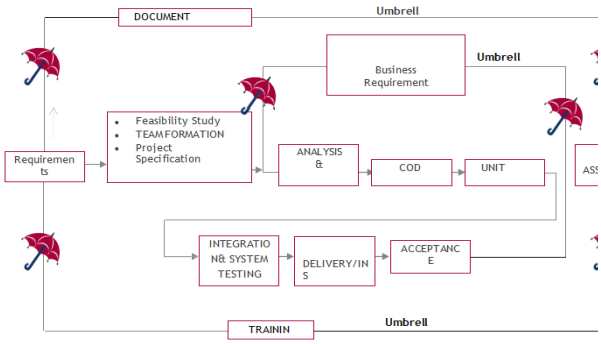
3.If user not casted vote then user can give vote to desire candidate by clicking link beside party name or candidate name.

4.Upon giving vote application will capture voter and candidate details and then encrypt the data and then store in Blockchain.

The implementation phase is less creative than system design. It is primarily concerned with user training, and file conversion. The system may be requiring extensive user training. The initial parameters of the system should be modifies as a result of a programming. A simple operating procedure is provided so that the user can understand the different functions clearly and quickly. The different reports can be obtained either on the inkjet or dot matrix printer, which is available at the disposal of the user. The proposed system is very easy to implement. In general implementation is used to mean the process of converting a new or revised system design into an operational one.

IV.ALGORITHM

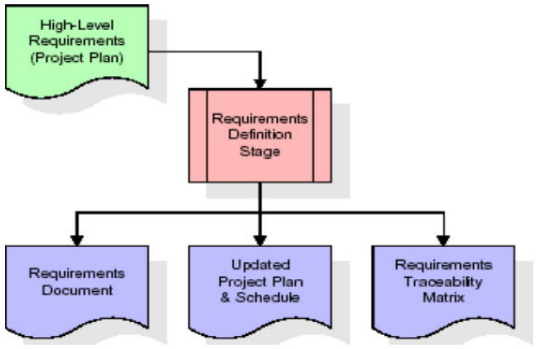
SDLC (Umbrella Model)



SDLC is nothing but Software Development Life Cycle. It is a standard which is used by software industry to develop good software.

Requirements Gathering stage:

The requirements gathering process takes as its input the goals identified in the high-level requirements section of the project plan. Each goal will be refined into a set of one or more requirements. These requirements define the major functions of the intended application, define operational data areas and reference data areas, and define the initial data entities. Major functions include critical processes to be managed, as well as mission critical inputs, outputs and reports. A user class hierarchy is developed and associated with these major functions, data areas, and data entities. Each of these definitions is termed a Requirement. Requirements are identified by unique requirement identifiers and, at minimum, contain a requirement title and textual description.



These requirements are fully described in the primary deliverables for this stage: the Requirements Document and the Requirements Traceability Matrix (RTM). The requirements document contains complete descriptions of each requirement, including diagrams and references to external documents as necessary. Note that

detailed listings of database tables and fields are not included in the requirements document.

The title of each requirement is also placed into the first version of the RTM, along with the title of each goal from the project plan. The purpose of the RTM is to show that the product components developed during each stage of the software development lifecycle are formally connected to the components developed in prior stages.

In the requirements stage, the RTM consists of a list of high-level requirements, or goals, by title, with a listing of associated requirements for each goal, listed by requirement title. In this hierarchical listing, the RTM shows that each requirement developed during this stage is formally linked to a specific product goal. In this format, each requirement can be traced to a specific product goal, hence the term requirements traceability.

The outputs of the requirements definition stage include the requirements document, the RTM, and an updated project plan.

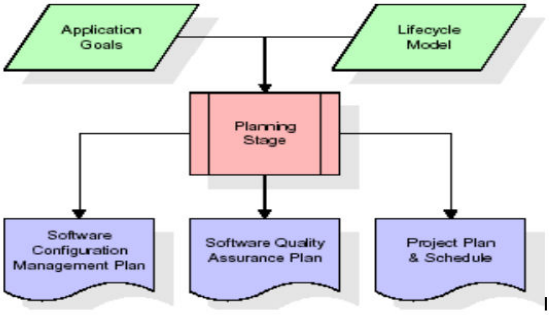
Feasibility study is all about identification of problems in a project.

No. of staff required to handle a project is represented as Team Formation, in this case only modules are individual tasks will be assigned to employees who are working for that project.

Project Specifications are all about representing of various possible inputs submitting to the server and corresponding outputs along with reports maintained by administrator.

Analysis Stage:

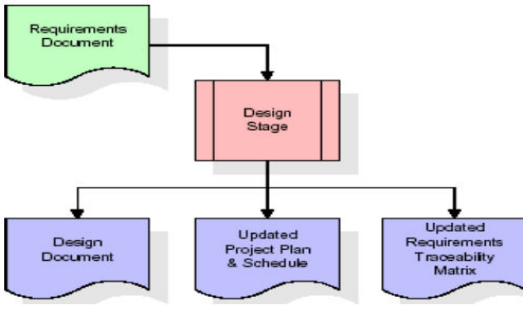
The planning stage establishes a bird's eye view of the intended software product, and uses this to establish the basic project structure, evaluate feasibility and risks associated with the project, and describe appropriate management and technical approaches.



The most critical section of the project plan is a listing of high-level product requirements, also referred to as goals. All of the software product requirements to be developed during the requirements definition stage flow from one or more of these goals. The minimum information for each goal consists of a title and textual description, although additional information and references to external documents may be included. The outputs of the project planning stage are the configuration management plan, the quality assurance plan, and the project plan and schedule, with a detailed listing of scheduled activities for the upcoming Requirements stage, and high level estimates of effort for the out stages.

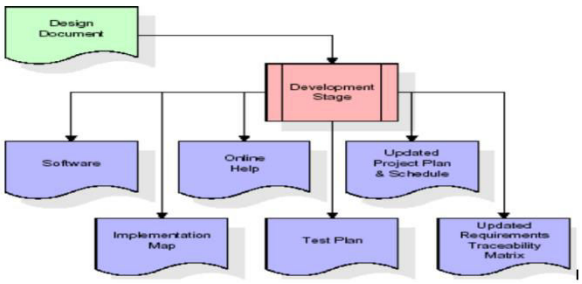
Designing Stage: The design stage takes as its initial input the requirements identified in the approved requirements document. For each requirement, a set of one or more

design elements will be produced as a result of interviews, workshops, and/or prototype efforts. Design elements describe the desired software features in detail, and generally include functional hierarchy diagrams, screen layout diagrams, tables of business rules, business process diagrams, pseudo code, and a complete entity-relationship diagram with a full data dictionary. These design elements are intended to describe the software in sufficient detail that skilled programmers may develop the software with minimal additional input.



When the design document is finalized and accepted, the RTM is updated to show that each design element is formally associated with a specific requirement. The outputs of the design stage are the design document, an updated RTM, and an updated project plan.

Development (Coding) Stage: The development stage takes as its primary input the design elements described in the approved design document. For each design element, a set of one or more software artifacts will be produced. Software artifacts include but are not limited to menus, dialogs, and data management forms, data reporting formats, and specialized procedures and functions. Appropriate test cases will be developed for each set of functionally related software artifacts, and an online help system will be developed to guide users in their interactions with the software.



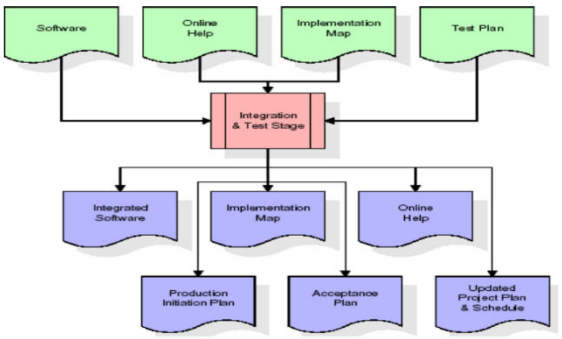
The RTM will be updated to show that each developed artifact is linked to a specific design element, and that each developed artifact has one or more corresponding test case items. At this point, the RTM is in its final configuration. The outputs of the development stage include a fully functional set of software that satisfies the requirements and design elements previously documented, an online help system that describes the operation of the software, an implementation map that identifies the primary code entry points for all major system functions, a test plan that describes the test cases to be used to validate the correctness and completeness of the software, an updated RTM, and an updated project plan.

Integration & Test Stage: During the integration and test stage, the software artifacts, online help, and test data are migrated from the development environment to a separate test environment. At this point, all test cases are run to verify the correctness and completeness of the software. Successful execution of the test suite confirms a robust and complete

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

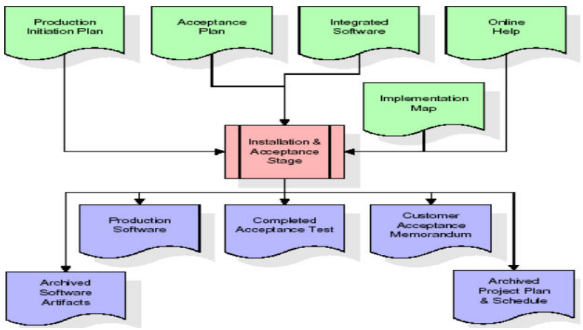
migration capability. During this stage, reference data is finalized for production use and production users are identified and linked to their appropriate roles. The final reference data (or links to reference data source files) and production user list are compiled into the Production Initiation Plan

During the integration and test stage, the software artifacts, online help, and test data are migrated from the development environment to a separate test environment. At this point, all test cases are run to verify the correctness and completeness of the software. Successful execution of the test suite confirms a robust and complete migration capability. During this stage, reference data is finalized for production use and production users are identified and linked to their appropriate roles. The final reference data (or links to reference data source files) and production user list are compiled into the Production Initiation Plan.



The outputs of the integration and test stage include an integrated set of software, an online help system, an implementation map, a production initiation plan that describes reference data andproduction users, an acceptance plan which contains the final suite of test cases, and an updated project plan.

Installation & Acceptance Test: During the installation and acceptance stage, the software artifacts, online help, and initial production data are loaded onto the production server. At this point, all test cases are run to verify the correctness and completeness of the software. Successful execution of the test suite is a prerequisite to acceptance of the software by the customer.After customer personnel have verified that the initial production data load is correct and the test suite has been executed with satisfactory results, the customer formally accepts the delivery of the software.



The primary outputs of the installation and acceptance stage include a production application, a completed acceptance test suite, and a memorandum of customer acceptance of the software. Finally, the PDR enters the last of the actual labor data into the project schedule and locks the project as a permanent project record. At this point the PDR "locks" the project by archiving all software items, the implementation map, the source code, and the documentation for future reference.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Deployment: Deployment in software and web development means pushing changes or updates from one deployment environment to another. When setting up a website you will always have your live website, which is called the live environment or production environment.

Maintenance: Outer rectangle represents maintenance of a project, Maintenance team will start with requirement study, understanding of documentation later employees will be assigned work and they will undergo training on that particular assigned category. For this life cycle there is no end, it will be continued so on like an umbrella (no ending point to umbrella sticks).

V.RESULTS

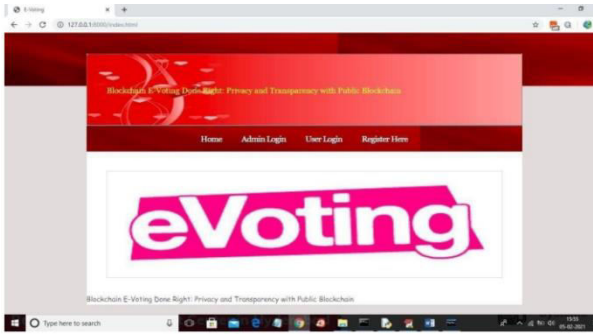


Fig:1,Home Page

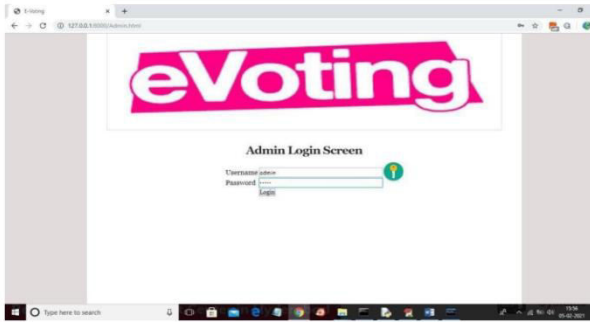


Fig:2,Login Screen

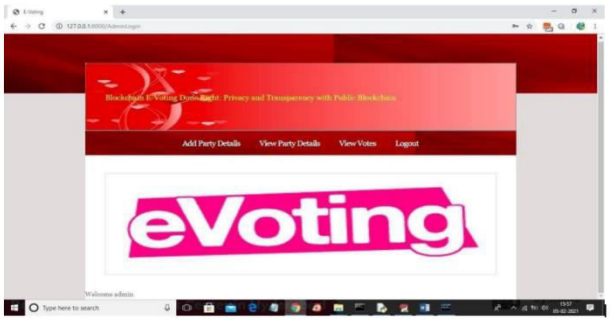


Fig 3AdminPage

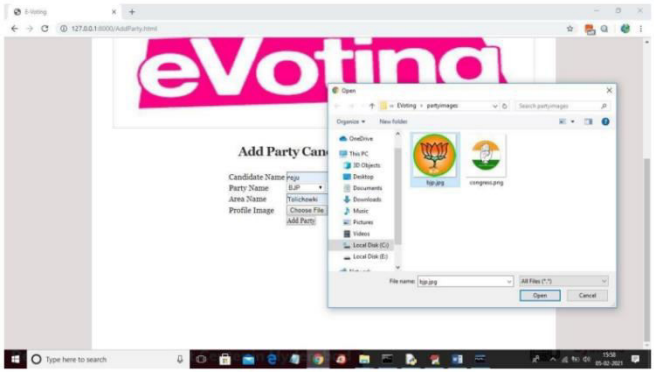


Fig 4 Adding Party Details Page

Fig 5 User Registration Page

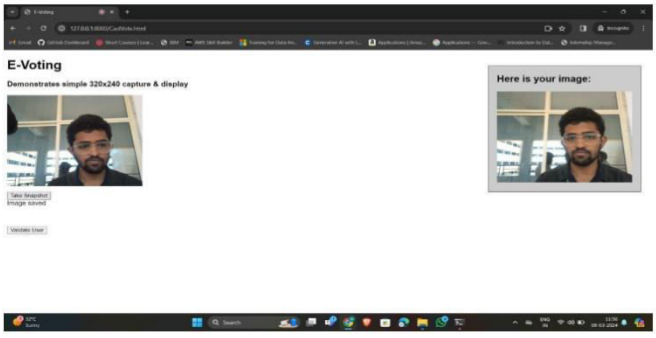


Fig 6 Vote Casting Page

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

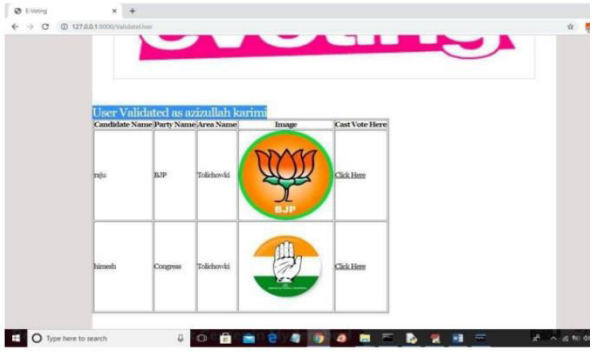


Fig 7.Vote Count Page

VI. CONCLUSION

In evaluating the performance of different blockchain networks for an electoral system, it becomes apparent that the choice between public and private blockchains hinges on various factors, including network transparency, decentralization, and speed. Public blockchains, such as Ethereum Ropsten, offer unparalleled transparency and accessibility, allowing anyone to view the transactional data in real-time. This openness fosters trust and accountability within the electoral process, as stakeholders can independently verify the integrity of the system. Despite slightly longer transaction times, the advantages of public blockchains in terms of data openness outweigh the minor differences in network speed.

Conversely, private blockchains, exemplified by platforms like Hyperledger Composer, may boast marginally faster transaction times due to reduced network congestion and centralized control. However, the inherent centralization of private blockchains compromises the decentralization and credibility of the electoral system. Private blockchains are operated and controlled by designated authorities, limiting access and oversight by external parties. This partial centralization undermines the foundational principles of blockchain technology, detracting from the overall trustworthiness of the electoral process.

In conclusion, while private blockchains may offer marginal advantages in terms of transaction speed, the transparency and decentralization afforded by public blockchains are paramount in ensuring the integrity and credibility of an electoral system. Ultimately, the choice of blockchain network should prioritize these fundamental principles to uphold the democratic ideals of fairness,transparency, and trust.

FUTURE ENHANCEMENTS

The future holds tremendous potential for the development and implementation of a secure voting system leveraging blockchain technology, integrated with advanced biometric authentication methods such as facial recognition and fingerprints. This innovative approach promises to revolutionize the electoral process by ensuring the integrity, transparency, and security of voting procedures. Here's an outline of the future scope for such a system.Implementing robust security protocols to safeguard the integrity of the voting process.Integrating biometric authentication methods such as facial recognition and fingerprints to verify the identity of voters securely.Develop in a decentralized infrastructure based on blockchain technology to distribute voting data across multiple nodes, ensuring

redundancy and resilience against cyber-attacks or system failures

REFERENCES

[1]N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, pp. 95-99, jul 2018.

[2]M. Pawlak, J. Guziur, and A. Poniszewska-Maranda, "Voting Processwith Blockchain Technology: Auditable Blockchain Voting System," inLecture Notes on Data Engineering and Communications Technologies, pp. 233-244, Springer, Cham, 2019.

[3]B. Singhal, G. Dhameja, and P. S. Panda, "How Blockchain Works," in Beginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[4]Agora, "Agora Whitepaper," 2018.

[5]R. Perper, "Sierra Leone is the first country to use blockchain duringan election - Business Insider," 2018.

[6]S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," tech.rep., 2008.

[7]G. Wood et al., "Ethereum: A secure decentralized generalized transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[8]S. Landers, "Netvote: A Decentralized Voting Platform – Netvote Project Medium," 2018.

[9]P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Lecture Notes in Computer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[10]Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE,"SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.

[11]O. Goldreich and Y. Oren, "Definitions and properties of zero knowledge proof systems," Journal of Cryptology of vol of cryptology vol 7 no 1 pp 1-32 1994