Blockchain-Enabled Electoral Process

[1]K. Devi Priya, [2*]Arvapalli Eswari, [3]Kodali karthik Sai, [4]Mallavarapu Vivek

[1]Associate Professor, Department of Computer Science and Engineering,
Lakireddy Balireddy college of Engineering, Mylavaram,
Andhra Pradesh-521230, India.
[2,3,4]Students, Department of Computer Science and Engineering,
Lakireddy Bali Reddy College of Engineering,
Mylavaram, Andhra Pradesh-521230, India
.
[1]kdevipriya20@gmail.com [2*]arvapallieswari02@gmail.com
[3]karthikkodalisr4@gmail.com [4]vivekmallavarapu3005@gmail.com

Abstract: There are numerous good effects of technology on our social lives. Creating an architecture that is globally connected around-the-clock makes it simple to access a wide range of resources and services. In addition, technology, such as the Internet, has fostered creativity and invention. Blockchain, the foundation of cryptocurrencies, is one example of the latest innovations. It is claimed that blockchain technology will revolutionise a number of current and future products and services. It is assuming a prominent role in many services as an equalising element to the existing parity between consumers and huge corporations/governments because of its immutability attribute and decentralised architecture. The blockchain has the potential to be used in electronic voting systems. Such a plan would aim to offer a decentralised architecture for the operation of conducting a fair election in order to determine the people's choice in creating a better democracy. Utilizing smart contracts, Ethereum stands out as an ideal choice for developing advanced, cost-effective, secure, transparent, and user-friendly e-voting systems. The Ethereum network, renowned for its consistency and widespread adoption, particularly excels in providing logical frameworks for smart contracts. Essential qualities of an e-voting system, including security against duplicate votes and complete transparency while safeguarding attendee privacy, align seamlessly with Ethereum's capabilities. Choosing Ethereum ensures a robust foundation for creating trustworthy and efficient e-voting solutions, addressing critical aspects of security, transparency, and user accessibility.

Keywords: Blockchain; Ethereum; Smart-contracts, E-voting.

1 Introduction

Voting, whether through traditional ballet-based methods or electronic voting (e-voting), forms the cornerstone of modern democracies. In recent times, a noticeable rise in voter apathy, particularly among the younger, tech-savvy demographic, has been observed. [1] As a potential remedy to this issue, e-voting has been advocated to specifically engage the younger generation. To establish a robust e-voting system, a set of functional and security requirements, encompassing aspects like transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability, and distribution of authority, are deemed essential. Blockchain technology operates on a distributed network comprising numerous interconnected nodes. Each node possesses an independent copy of the distributed ledger, documenting the comprehensive transaction history of the network. Crucially, there exists no singular authority governing the network; instead, transactions are accepted if a majority of nodes reach consensus. This decentralized network ensures user anonymity [2]. Initial analysis of blockchain technology, inclusive of smart contracts, indicates its suitability as a foundation for e-voting, presenting the potential to enhance the acceptability and reliability of the process. Several papers, including this one, have explored this concept. Blockchain, a form of Distributed Ledger Technology (DLT), ensures the immutability and transparency of digital assets through decentralization and cryptographic hashing. As outlined in [3], key features of blockchain include a distributed ledger preventing single points of failure, allowing anyone with distributed control to add new transactions, the creation of blocks based on previous block details, and the pivotal role of consensus

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_12

algorithms in constructing and processing transactions within a new block. The paper's aim is to establish a voting system leveraging Blockchain technology to ensure transparency and security in the electoral process. Leveraging blockchain for e-voting presents clear advantages, including enhanced transparency through open and distributed ledgers, inherent voter anonymity, heightened security against Denial-of-Service Attacks, and the immutability of records, ensuring the integrity of the voting process and individual votes. While existing literature focuses on the positive impacts of blockchains on e-voting requirements, there is a notable gap in addressing implementation challenges and limitations of current blockchain and smart contract technologies, especially for large-scale voting systems. This paper aims to explore both the possibilities and constraints of implementing an e-voting scheme using blockchain technology, considering the unique challenges posed by voting environment. Unsuitable for critical scenarios. Another platform, https://electionrunner.com/, allows users to create and share elections but lacks confidence in the central authority of Electronic Runner Inc. In contrast, a well-researched study proposes a robust blockchain-based electronic voting system, considering voter anonymity and privacy. While insightful, the paper primarily discusses Bitcoin and Zerocoin as currencies and lacks detailed implementation information.to communication and fostering a more empathetic and approachable environment through the transformational potential of technology [4].

2 Related Work

Establish a secure voting environment and demonstrate the viability of a blockchain-based electronic voting system [5], emphasizing accessibility for everyone via computers or mobile devices. The objective is to empower individuals to engage in administrative decisions, fostering transparency in public opinion for managerial and legislative bodies. This democratization aligns with the ideals of true direct democracy, with the potential to mitigate election corruption, particularly in smaller towns and corrupt regions. Conventional large-scale elections pose challenges like high costs and logistical issues such as geographically dispersed polling places and absentee voters. E-voting emerges as a potential solution, with Estonia serving as a pioneer in online voting since 2003. However, centralized systems like Estonia's are vulnerable to DDoS attacks and potential malicious actions by administrators [6].Switzerland, renowned for its democratic values, is exploring electronic voting to engage voters at the age of 18. Despite various online platforms attempting to address voting concerns, like followmyvote.com and strawpoll.me, comprehensive solutions are lacking. Our project aims to contribute to a more inclusive and reliable democratic process by addressing the limitations of current models.Different e-voting platforms exhibit varying security features, with some compromising voter authentication, vote duplication, and non-repudiation for user convenience, making them unsuitable for critical scenarios. Another platform, https://electionrunner.com/, allows users to create and share elections but lacks confidence in the central authority of Electronic Runner Inc.In contrast, a well-researched study proposes a robust blockchain-based electronic voting system, considering voter anonymity and privacy. While insightful, the paper primarily discusses Bitcoin and Zerocoin as currencies and lacks detailed implementation information.Our project's main goal is to overcome these challenges by introducing a secure e-voting system on a smaller scale, focusing on university elections like student councils, department chairs, and university rectors. The unique aspect is the integration of these elections with Ethereum blockchain technology. Limited scholarly papers on Ethereum blockchain and e-voting exist, often suggesting complex methods unsuitable for IoT applications. The project developed Ethereum smart contracts for vote counting and verification, ensuring voter anonymity through hash values, with recognition of personal authentication and legal regulations as distinct issues beyond the current scope.Numerous scholars have expressed interest in conducting innovative research in the field of block chain technology, as it is becoming necessary for numerous applications. Suggested a permissioned block chain election system that makes use of smart contracts to guarantee election security and economy. The use of blockchain-based voting solutions at many levels, including business, community, city, and national voting, was recorded in . The benefits and difficulties of blockchain-enabled voting (BEV) were also covered. The approved voters can use digital currency to cast a ballot in BEV as well. Voting on a block chain creates tamper-proof audit trails, making it an ideal method for casting ballots. Examined the I-voting systems in several nations in. A potential electronic voting protocol is put out that makes use of the blockchain to function as an open voting booth.

The paper makes two significant contributions they are as follows,. It introduces an e-voting scheme utilizing blockchain technology that aligns with essential e-voting properties. This innovative approach not only adheres to the guidelines set by the Election Commission of India but also introduces a level of decentralization, empowering voters with greater control over the process[7]. The proposed scheme seeks to balance regulatory compliance with the benefits of blockchain in enhancing the e-voting experience.The paper engages in a comprehensive discussion on the challenges associated with implementing this e-voting proposal. It critically examines the limitations of the underlying platforms, namely blockchain and smart contracts, shedding light on potential obstacles and constraints. By addressing both the proposal's novel features and the practical hurdles in implementation, the paper offers a holistic exploration of the landscape surrounding blockchain-based e-voting systems.

3 Proposed methodology

In our blockchain-based electronic voting system, leveraging distributed ledger technology ensures unparalleled transparency and security. Through cryptographic encryption, each vote is transformed into a tamper-proof transaction recorded on the blockchain. Smart contracts enforce predefined voting rules, ensuring accuracy and anonymity while eliminating the risk of manipulation. The decentralized nature of the blockchain prevents any single entity from controlling the process, fostering trust among voters. Immutable and transparent, the system offers a verifiable record of every vote cast, enhancing the integrity of democratic elections and paving the way for a more accessible and resilient electoral process in the digital age. Architecture of the E-voting process shown in figure 1. Electronic voting systems, known as 'e-voting mechanisms', have undergone thorough examination in both commercial and academic spheres.

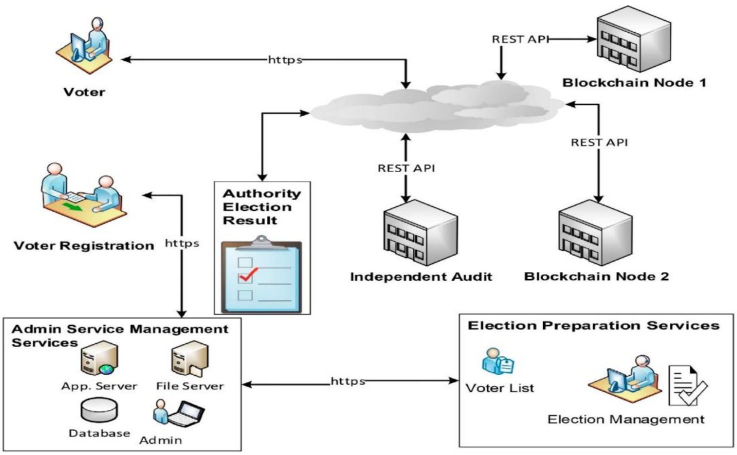

Fig 1: E-voting process

These mechanisms, designed to facilitate the casting and counting of votes, have been a focal point of study, exploring their application and effectiveness in modern electoral processes, as in fig 2. Research efforts have spanned across both industry and academia, reflecting a widespread interest in leveraging electronic means for enhancing the efficiency and accuracy of voting procedures.

Design Properties

Ensuring Integrity in E-Voting Protocols: A Comprehensive Analysis. In the realm of electronic voting (e-voting), a set of fundamental properties serves as the bedrock for designing a robust and trustworthy protocol. These properties encompass the dimensions of fairness, eligibility, privacy, verifiability, coercion-resistance, and the distinct inclusion of forgiveness.[8]

Fairness:

A fundamental principle dictates that no preliminary results should be available until the completion of the voting process. This precautionary measure prevents any unwarranted influence on remaining voters, guaranteeing that each person's decision is made autonomously and free from external pressures. .

Eligibility:

Establishing eligibility is paramount, stipulating that only those entitled to vote are permitted to do so, and they must cast their vote only once. Authentication becomes pivotal in this context, as voters need to authenticate their identity before being granted the privilege to participate in the electoral process.

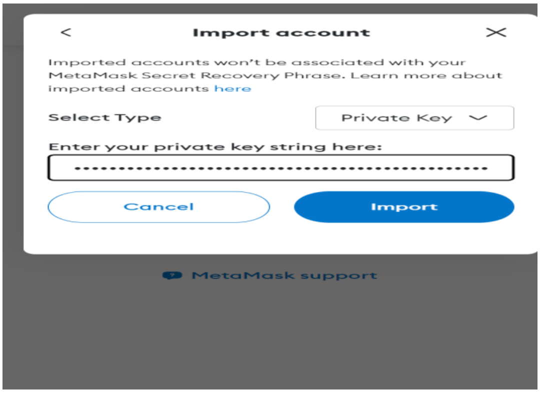

Fig- 2 Importing ganache account to MetaMask

Privacy:

Preserving voter privacy is a cornerstone, asserting that an individual's vote should remain confidential and undisclosed to any external entity .In traditional, non-electronic voting systems, this is achieved through physical measures that shield the voter from prying eyes.

Verifiability:

The property of verifiability is crucial, ensuring that all stakeholders have the means to verify whether their votes have been accurately counted. This bifurcates into individual verifiability, enabling voters to confirm that their votes have been tallied, and universal verifiability [9], which mandates that anyone can scrutinize and confirm the published election outcome.

Coercion-Resistance:

A robust e-voting protocol must be resistant to coercion, implying that a coercer should be unable to discern whether a voter cast their ballot as instructed. However, acknowledging the practical challenges, full coercion resistance might be unattainable solely through technological means in remote e-voting [10]. While the project strives to incorporate all the mentioned attributes, it adopts a practical approach to coercion resistance, recognizing the difficulties in achieving this solely through technological means in remote e-voting. In lieu of this, the protocol introduces the inventive concept of Forgiveness, offering a practical compromise that strengthens the system against undue influence and coercion. This pragmatic approach ultimately enhances the overall integrity of the e-voting process.

Registration:

The initial step involves voter registration, where each valid voter is allocated a block in the blockchain and this block contains a private key which is then shared with the user and this private key is used for subsequent authentication in the MetaMask during the voting. To maintain anonymity, voters receive enough ethers for a single transaction, and both their public address (User Id’s) and private key are kept confidential. This meticulous process establishes a foundation for secure and discreet voting [11].

Fig -3 Displaying the Candidate Results.

Authentication:

The voting process commences with authentication, wherein each eligible voter utilizes their assigned address and private key to verify their identity in the MetaMask during the voting process . Voters input their private key as authentication credentials, granting them the privilege to cast their votes upon successful validation. This robust authentication mechanism safeguards the integrity of the voting system.

Voting:

Once authenticated, voters utilize the Frontend application to select a candidate from the available options. Each voter is granted a single opportunity to cast their vote, achieved by invoking a function call to the deployed smart contracts, specifying the candidate's ID (Private Key). This ensures a streamlined and controlled voting experience.

The final phase involves the declaration of results shown in fig 3. The success of a block transaction relies on its confirmation by any miner and acknowledgment by all miners in the network. This multi-step validation process ensures the accuracy and consensus of the recorded votes, culminating in a secure and verifiable electoral outcome. The systematic flow of activities within this voting system architecture, from registration through authentication, voting, and results, collectively establishes a comprehensive and resilient framework that addresses key aspects of security, anonymity, and transparency in the electoral process [12]. These results are:

1. Transparent and Tamper- Proof
2. Automatically Tallied
3. Decentralized Verification
4. Anonymous
5. Private
6. Real-Time Accessibility
7. Immutable Audit Trail

8. Reduced Fraud and Manipulation

4 Experimental Setup

The experimental setup of our project deal with some of the major components of the model like ganache, Node server, meta mask, smart contracts, Mongo DB [13].

Ganache:

Ganache serves as an Ethereum development tool—a personal blockchain emulator tailored for testing. Specifically designed for developers, it offers a local environment for deploying and interacting with smart contracts, eliminating the necessity for a live Ethereum Network during the testing and development phase. Ganache, shown in fig 4, offers a graphical user interface and command-line interface, allowing users to simulate various blockchain scenarios, control account balances, and inspect transaction logs. With features like block exploration and integrated tools, Ganache streamlines the development and debugging process, enabling developers to efficiently create, test, and deploy decentralized applications on the Ethereum blockchain in
a secure and controlled environment.

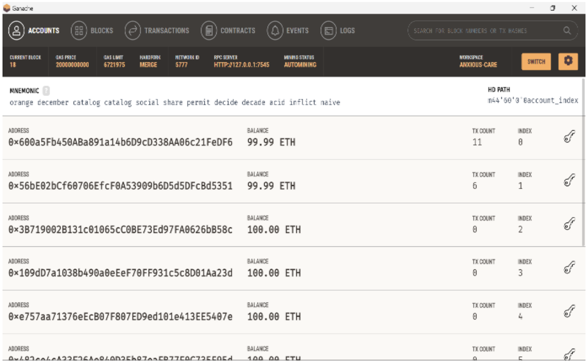

Fig – 4 Ganache Work Space

Smart Contracts:

Smart contracts are self-executing programs, shown in fig 5, with predefined rules and conditions encoded on blockchain platforms, most notably Ethereum. These decentralized agreements automate, verify, or enforce

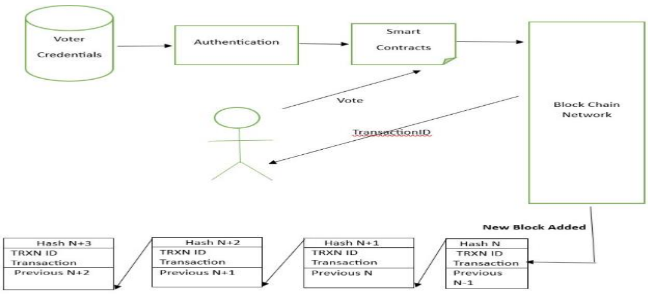

Fig- 5 Flow Chart of Smart Contracts

contractual obligations without intermediaries. Written in languages like Solidity, they run on blockchain nodes, ensuring transparency, security, and immutability. Smart contracts trigger actions when predefined conditions are met, enabling trustful and tamper-resistant transactions. Widely used in decentralized finance (DeFi), supply chain, and voting systems, smart contracts enhance efficiency and reduce fraud risks.

Node Server:

A Node.js server is a powerful runtime environment that enables server-side execution of JavaScript code. Based on the V8 JavaScript engine, Node.js facilitates scalable and efficient network applications. Its non-blocking, event-driven architecture

allows handling multiple concurrent connections with low overhead, making it particularly suitable for real-time applications. Node.js employs an event loop that efficiently manages asynchronous tasks, enhancing performance and responsiveness making it an excellent choice for applications with a large number of concurrent connections, such as chat applications, real-time collaboration tools, and streaming services. Overall, Node.js serves as a key technology for building scalable and responsive server-side applications in the ever-evolving landscape of web development.[13]

Mongo DB:

MongoDB stands as a highly utilized NoSQL database management system, in fig 6, crafted for the storage and retrieval of substantial volumes of unstructured or semi-structured data. It distinguishes itself through its adaptability, scalability, and proficiency in managing varied data types, rendering it well-suited for contemporary and dynamic applications. Employing a document-oriented model,

MongoDB stores data in a flexible manner. A notable this well-organized structure made it easier to integrate with well-known machine learning frameworks and made the process of training and evaluating the model easier. Quality control was prioritized

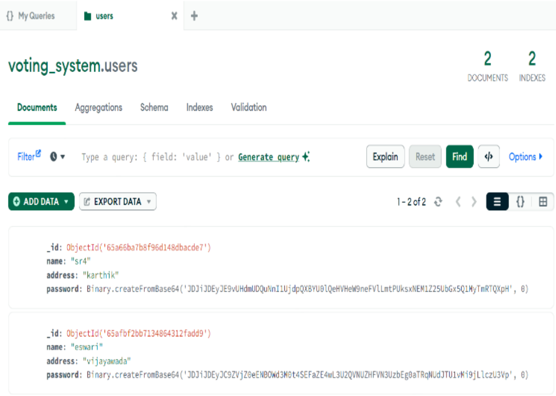

Fig-6 MongoDB for Voting Systems

Heavily during the data preparation stages. To make sure that the extracted features correctly depicted the sign motions, human checks of a portion of the data were included as part of continuous feedback loops. Iterative refinement was employed to address any inconsistencies or anomalies, guaranteeing that the dataset remained dependable and representative of the wide range of sign language expressions of distributing data across multiple servers to cater to expanding datasets. This attribute positions MongoDB as an outstanding option for applications with dynamic and growing data needs. In the realm of database management systems [11-13], MongoDB is esteemed for its capability to handle diverse data structures and its responsiveness to the evolving demands of modern applications. The document-oriented approach not only enhances data representation but also facilitates efficient retrieval and manipulation of complex information. MongoDB's emphasis on scalability, combined with its open-source nature, underscores its relevance in meeting the challenges posed by the data-intensive landscape of contemporary software development.

Meta Mask:

MetaMask operates as a dual-purpose tool, serving as both a cryptocurrency wallet and a browser extension. Its primary function is to facilitate user interactions with decentralized applications (DApps) on the Ethereum blockchain. Functioning as a crucial intermediary connecting browsers and the Ethereum blockchain, MetaMask, in fig 7, ensures seamless transaction execution and efficient management of digital assets. Users can securely store and transfer not only Ether but also ERC-20 tokens, all within the confines of a user-friendly interface Beyond its wallet capabilities, MetaMask extends its utility by acting as an Ethereum identity provider. This added functionality enhances MetaMask's significance, allowing users to engage securely and efficiently with the Ethereum blockchain and its diverse range of decentralized applications. In summary, MetaMask stands as a versatile tool, seamlessly integrating cryptocurrency management, browser extension capabilities, and Ethereum identity provision to offer users a comprehensive and user-friendly experience within the decentralized ecosystem. MetaMask enables users to securely perform transactions on the Ethereum blockchain. Users can seamlessly send, receive, and manage Ether and ERC-20 tokens, fostering efficient interactions with decentralized applications.

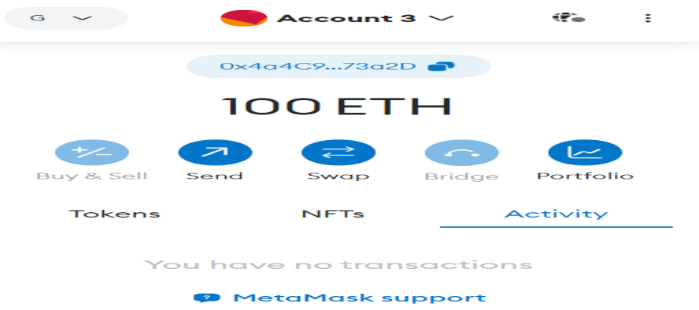

Fig 7- MetaMask accounts

Working:

To commence this, the initial step involves launching Visual Studio Code and configuring the necessary paths. The initial command, "cd blockchain," is then executed to navigate to the blockchain directory, housing pertinent components such as the truffle file and smart contracts. Subsequently, the "truffle compile" command is employed, compiling essential files and generating a build file. This streamlined process ensure the proper setup, in fig 8, and compilation of blockchain-related components, facilitating a structured foundation for the project within the Visual Studio Code environment. Next in the process is activating Ganache, serving as the

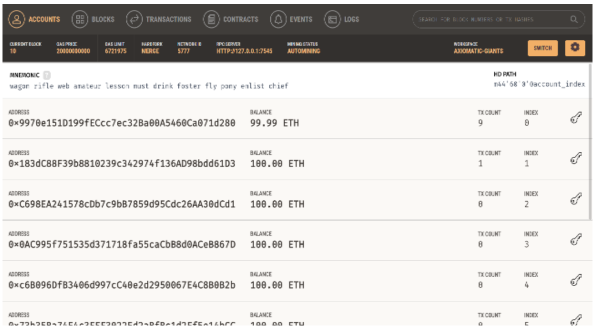

Fig- 8 Ganache Workspace

blockchain provider. Following Ganache activation, a new workspace is created by exporting the truffle-config file, housing the Ethereum API, Returning to Visual Studio Code, another command is entered: "truffle migrate --reset." This command initiates the compilation and deployment of various smart contracts developed for the project onto the blockchain. Noteworthy is the incurring cost, termed gas cost, associated with deploying these contracts, constituting the transaction fee for each executed operation. This command initiates the compilation and deployment of various smart contracts developed for the project onto the blockchain. Noteworthy is the incurring cost, termed gas cost, associated with deploying these contracts, constituting the transaction fee for each executed operation. In the blockchain ecosystem, every action takes the form of a transaction, and users are charged ethers for each transaction, emphasizing the importance of managing resources efficiently. This integral step ensures the deployment and execution of the project's smart contracts while underscoring the financial implications tied to blockchain transactions. Ganache further enhances its utility by offering a batch of 10 pre-configured accounts every time users access the application. This feature ensures a readily available pool of accounts with predefined balances for developers to simulate various blockchain scenarios efficiently. By leveraging Ganache's user-friendly interface and robust functionality, our project benefits from a secure and controlled blockchain environment tailored to the intricacies of Ethereum development The use of Ganache in our application underscores our commitment to a thorough testing and development process, harnessing the capabilities of this third-party web application to streamline smart contract deployment and interaction while ensuring optimal resource availability for developers. Each account that is provided by ganache must be linked to an E-wallet so that the transactions that are performed on the blockchain can be performed through the wallet that is connected to the blocks of our blockchain. The initial account is consistently linked to the admin, facilitating essential administrative functions such as adding voters and contestants to the blockchain. These transactions, constituting various actions, incur a transaction fee termed "gas cost." This fee covers the expenses associated with executing tasks on the blockchain. Notably, the admin's account bears this cost during the performance of administrative duties. The remaining accounts within Ganache are available for allocation to individual voters, ensuring a streamlined and organized process for managing interactions and transactions within the blockchain-based application. The administrator plays a pivotal role in our system, not only overseeing voter registration but also directly registering contestants from diverse parties onto the blockchain. Each contestant is assigned a dedicated block within the blockchain. To facilitate these transactions, MetaMask, a cryptocurrency wallet and browser extension, acts as an intermediary between browsers and the Ethereum blockchain. MetaMask empowers users to seamlessly engage with decentralized applications (DApps), in fig 10, enabling actions such as block allocation to voters or contestants. Noteworthy is the fact that every operation incurs a gas cost, serving as a transaction fee on the blockchain. Users are responsible for covering these fees, deducted from their accounts, as transactions are executed through the MetaMask e-wallet, ensuring a secure and transparent process for managing digital assets and interactions. Operating through the Node Package Manager (npm), the command triggers the execution of predefined script labelled "dev" within the project files. The result is the generation of a localhost link. This link, which denotes the local development environment, must be copied and subsequently pasted into the URL, in fig 11, bar of any web browser. By doing so, developers gain access to the live instance of their application, streamlining the testing and debugging process within a controlled local server environment. The utilization of “npm run dev” enhances the efficiency of web development, providing a seamless and convenient means to preview and troubleshoot applications in real-time before deployment. After turning the server on, we need to open another power shell(terminal) and set the path to blockchain directory by using the command “cd blockchain” and after setting up the path we need to enter the command “npm start” to start the localhost and the application will be opened in the primary browser that we have selected. The below is the landing page which contains the admin login and user login options. Exclusive access to the admin-login feature is granted solely to the administrator. The login credentials for the admin are encoded in JavaScript, enabling secure login without the need for database connectivity. Users, on the other hand, utilize the “Registration and User Dashboard” option, which serves a dual purpose for both logging in and signing up. This versatile option caters to user authentication needs, providing a seamless experience for users to either log in or register for access to the application's features. The admin can login to the admin’s account by using the admin credentials that are hard coded into the java script. After logging into the admin’s account, the admin will have the following functionalities;

The admin can create a new election.

The admin can add the candidates that are going to contest in the election.

The admin can view the results of the elections held. The administrator has the capability to incorporate new candidates into the system by inputting relevant candidate details such as name and affiliated party.

To add a candidate, the administrator must link their MetaMask account with the browser. Importing the administrator's blockchain data into MetaMask enables the addition of contestants participating in the elections. Initiating a transaction is pivotal for allocating a blockchain block to a contestant. The successful execution of this transaction necessitates, the administrator to synchronize their MetaMask account with the browser, ensuring a seamless interaction between the administrator's MetaMask account and the blockchain for adding contestants to the electoral process. The candidates that have been added by the admin can be visible to the voters during the voting phase. On the other hand, the users can directly log in to the account using their credentials. After logging in the users will be able to see the elections that are being held. The user can then select the particular election and click on the election. After clicking on the

election, the user won't be able to see the candidates that are contesting in the election because the candidate isn't authenticated with the private key of the block allocated to them. the user will only be able to see a blank screen until he/she imports their block using the MetaMask extension. The user has to import his/her block using the MetaMask account. The user has to fill in the private key, fig 9, of the block allocated to him/her.

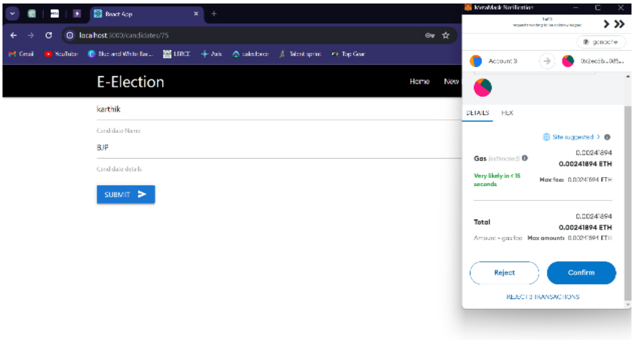

Fig – 9 Adding New Member

By using this private key, the user's block is connected to the meta mask account of the user. On the day of the election the user can log into the user's account that he/she has previously created and can go into the voting section which will only be visible when the admin has commenced the voting on the voting day. The voter can now choose the candidate and cast his/her vote for that particular candidate. when the voter casts the vote, the vote will be casted has a blockchain transaction which will cost some transaction fees also known as gas cost. Here some ethers from the user's account will be transferred to the candidate's block. This is basically a transaction and hence some gas cost will be charged and the vote will casted on to the selected candidate Once a user completes voting for a candidate, attempting to vote again, whether for the same candidate or another, will prove futile. This is attributed to the voting page creation process, where the web browser establishes a session and collects essential cookies.

After casting a vote, the page undergoes a reload, triggering the creation of a new session. In this renewed session, the necessary cookies from the prior session are unavailable, rendering the page devoid of the resources required for voting. Consequently, the vote count remains unaffected as the absence of essential cookies, in the new session prevents any further casting of votes. This mechanism ensures the integrity of the voting process by restricting users from submitting multiple votes and reinforces the credibility of the candidate Vote.

In this way all the voters can cast their vote on the voting day and at the end of the day the admin can display all the voting details like;

i. Number of voters that have taken part in voting.
ii. Number of votes that have been casted for each candidate.
iii. The winner of the election etc.

Here all the transactions that are taking place, in fig 10, can be viewed on the public ledger which is tamper proof and no user(block) can modify the results or tamper any transaction that has been performed.

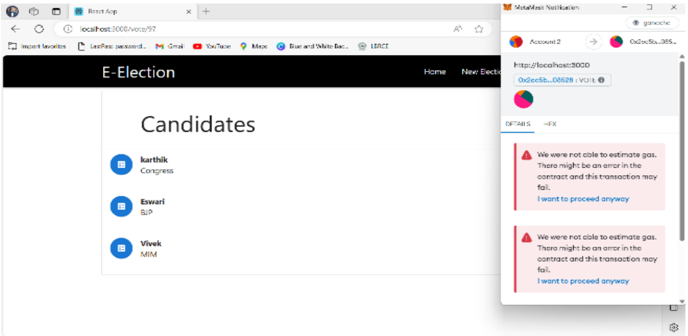

Fig-10 Votes Casted for each candidate

Comparisons

Structuring an electronic voting system which fulfills the legitimate requirements of representatives has been a challenge for a long time. Conducting the free, systematic and impartial election is the vital goal of every democracy nation. Every country follows a different voting system from old paper ballot system to electronic voting system. Network Vulnerabilities2. Voter Authentication Blockchain technology's decentralisation, anonymity, and non-tampering properties have made it a better contender for overcoming electronic voting's concerns in the recent years. In this research, we propose a Blockchain-based online voting system. DISADVANTAGES: 1. User Scalability2. Initial Setup Costs. A Transaction or a particular event takes place which is being recorded over the blockchain network. After a particular event occurs for example, a vote made by a person, this event is verified and in blockchain, the process of verification is done by the network of computers.

5 Conclusion And Future Works

The implementation of our proposed smart contract has successfully elevated the concept of e-voting by integrating it into the blockchain, mitigating inherent issues present in traditional e-voting systems. Leveraging the Ethereum network and blockchain structure, our trials have demonstrated the adaptability of blockchain technology and its security measures, particularly utilizing immutable hash chains, within the realm of polls and elections. This achievement not only marks a revolution in e-voting but also extends the potential applications of blockchain to various aspects of human life. The significance of Ethereum and smart contracts in this venture cannot be overstated. These technologies, serving as groundbreaking developments in the blockchain domain, have surpassed the initial perception of blockchain merely

as a cryptocurrency. Instead, they have transformed it into a versatile solution addressing numerous challenges in the modern internet landscape, potentially fostering global adoption of blockchain technology. While e-voting remains a debated topic, conventional solutions grapple with security, privacy, usability, and scalability issues. In contrast, our implementation of blockchain-based e-voting, utilizing smart contracts on the Ethereum network, effectively tackles various security concerns. These encompass voter privacy, vote integrity, verification, non-repudiation, and transparency during the counting process. Despite these achievements, certain aspects, such as personal-level voter authentication (beyond the account level), necessitate additional mechanisms outside the blockchain scope. Integration of supplementary measures, such as biometric factors, becomes crucial to address these requirements. Our work signifies a breakthrough in secure and transparent e-voting, emphasizing the ongoing need for research and development to enhance the multifaceted nature of blockchain-based solutions.

References

[1] Xu, M., Chen, X. & Kou, G. A systematic review of blockchain. FinancInnov5, 27 (2019). https://doi.org/10.1186/s40854-019-0147

[2] Fran Casino, Thomas K. Dasaklis, ConstantinosPatsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues”, Telematics and Informatics, 36, pp.55 81, 2019.and open issues”, Telematics and Informatics, 36, pp.55 81, 2019.
[3]https://www.britannica.com/topic/electronic-voting Types of Voting
[4] FriOrik b. Hjalmarsson; Gunnlaugur K. HreiOarsson; Mohammad Hamdaqa; GishHjalmtysson “Blockchain-Based E-Voting System” IEEE 11th International Conference on Cloud Computing (CLOUD)2018.
[5] NirKshetri and Jeffrey Voas, “Blockchain-Enabled E-Voting”, in IEEE Software,doi: 10.1109/MS .2018.2801546
[5] Taş, R.; Tanrıöver, Ö.Ö. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. *Symmetry* **2020**, *12*, 1328. https://doi.org/10.3390/sym12081328
[6] Fridrik .P. Hjalmarsson, Gunnlaugur .K. Hreidarsson, “Blockchain- Based E-Voting System”, in School of Computer Science Reykjavik University, Iceland
[7] Ahmed Ben Ayed, “A Conceptual Secure Blockchain- Based Electronic Voting System”, in International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3
[8] Freya Sheer Hardwick, ApostolosGioulis, Raja NaeemAkram, and KonstantinosMarkantonakis, “E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy”, in ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom
[9] BitCongress. Control the world from your phone. [Online]. Available: http://www.bitcongress.org/BitCongress\ Whitepaper.pdf
[10] Vairam, S. Sarathambekai and R. Balaji, "Blockchain based Voting system in Local Network," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 363-366, doi: 10.1109/ICACCS51430.2021.9441912
[11] A. Mendon, B. Manoj Votavat and A. Lodh, "Blockchain based e-voting system," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 1785-1792, doi: 10.1109/ICICICT54557.2022.9918010.
[12] V. Gupta, J. N. Singh, S. I. Khan and A. Chabaque, "Blockchain-Based Electronic Voting System," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 2049-2053, doi: 10.1109/ICAC3N56670.2022.10074384.
[13] S. Drakshayani, U. Vijayalakshmi, S. R. Sri, A. Srivani and A. Vyshnavi, "Online Voting System Using Blockchain," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 886-891, doi: 10.1109/ICEARS53579.2022.9752044.