BLOCKCHAIN-BASED VOTING SYSTEMS: REVOLUTIONIZING DEMOCRATIC PROCESSES FOR SECURE, EFFICIENT, AND TRANSPARENT ELECTIONS

Abstract

Voting plays a vital role in democratic societies, enabling citizen participation in decision-making. However, traditional voting methods face challenges like geographical constraints, fraud threats, and operational inefficiencies. The emergence of blockchain technology presents an incredible opportunity to address these issues and enhance the security, efficiency, and transparency of voting systems. This chapter explores the concept of blockchain-based voting systems, utilizing the decentralized and irreversible nature of blockchain to overcome the limitations of previous techniques. By leveraging transparent and tamper-resistant ledgers, integrity and transparency is ensured by blockchain technology of the voting process. Smart contracts on the blockchain automate critical voting procedures, such as candidate registration, voter identification, and result tabulation, streamlining the process and reducing human error. Furthermore, blockchain-based voting systems enhance accessibility by enabling remote ballot casting through internet platforms. Cryptographic approaches can be employed to protect voter privacy while ensuring verifiability. The potential of blockchain-based voting systems to revolutionize democratic processes lies in harnessing the advantages of blockchain technology, including immutability, transparency, and decentralization. These technologies can enable secure, efficient, and transparent elections, instilling confidence among voters and stakeholders. As blockchain technology advances, it becomes imperative to investigate its application in voting systems, aiming to create a more inclusive, participatory, and resilient democratic landscape.

Keywords: Blockchain, Voting System, Wishper, Markle Tree, Consortium, Hybrid, Hash

Authors

Muntazir Mehdi
B.Tech Scholar
Department of IT
Panipat Institute of Engineering and Technology
Samalkha, Panipat, India.

Vipin Tomar
Assistant Professor
Department of CSE
Panipat Institute of Engineering and Technology
Samalkha, Panipat, India.

Rajender Kumar
Associate Professor
Department of CSE
Panipat Institute of Engineering and Technology
Samalkha, Panipat, India.

I. INTRODUCTION

Blockchain technology has evolved as a game-changing concept, capturing global attention and reinventing industries worldwide. It is a distributed ledger system that allows for secure and transparent storage of information and transport. Blockchain first gained prominence as the underlying technology underpinning crypto-currencies like Bitcoin. Moreover, it's possible applications goes far beyond the arena of digital money. A blockchain comprises of a serial blocks in which every block comprises of a list of transactions or data. All such blocks are bonded with one another using cryptographic hashes to generate an immutable and non tamper- able chain. As soon as a transaction or data piece get recorded on the blockchain, it is nearly hard to change or erase it without the network's members' agreement. The decentralization of blockchain technology is one of its distinguishing qualities. A blockchain operates on a peer-to-peer network, as opposed to traditional centralized systems where a central authority regulates and verifies transactions. Each network participant, known as a node, keeps a copy of the blockchain and collaborates to verify and validate transactions. This decentralized nature lessens the need for intermediaries, lowers the danger of fraud, and increases transparency and confidence. Blockchain technology has the potential to be used in a variety of industries, including finance, supply chain management, healthcare, and voting systems. Traditional voting techniques involve issues such as geographical limits, potential fraud, and inefficiency. However, by exploiting the unique characteristics of blockchain, a new generation of voting systems that address these constraints and herald in a new era of secure, efficient, and transparent elections can be established [1].

1. **Blockchain:** A distributed database which is highly encrypted, and records data in the form of a digital ledger for any transaction is said to be operating as a Blockchain. An interesting fact of Blockchain is its digital ledger which can be accessed across multiple computer that are located at several distinct geographical locations. The financial service sector is becoming highly disrupting due to Blockchain and also underpins the field of digital currency like bitcoin. Blockchain records transactions between two persons as distributed and open ledger. It is best because all the transactions can be recorded as permanent or verifiable. Blockchain is created via using open-sources and hence, as per the requirements of different industries a customized set of blockchain versions can be developed [2].

2. **Working of Blockchain :** Every new transaction that has to added in existing chain is needed to be verified by every participant of the parent Blockchain ecosystem. To perform such verification and validation some specific algorithm are applied. For every ecosystem of Blockchain each validation and verification system differs. All the transactions for a particular system are bundled together as blocks. This block is communicated with every participating entities of the ecosystem. Every chained block is comprised of hash and digital fingerprint which is unique from the preceding block.

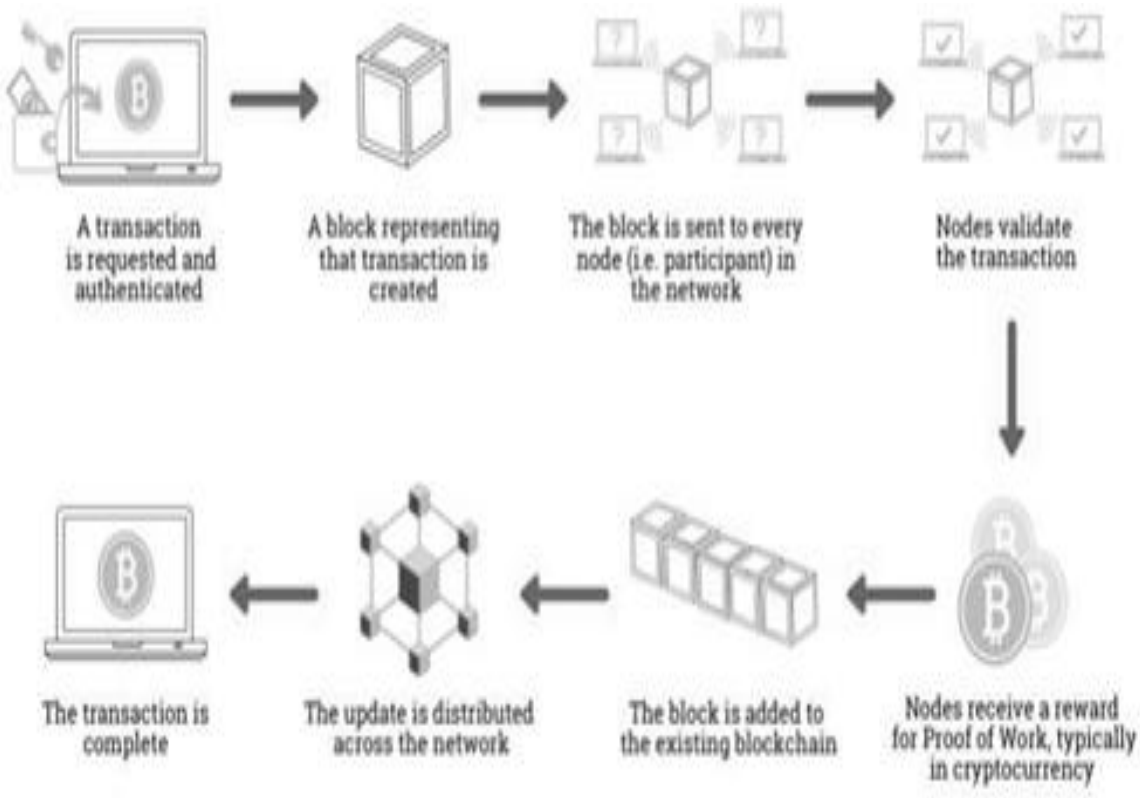

Figure 1: Blockchain Transaction

Figure 1 represents occurrence of Blockchain transactions via a detailed example. If Bob wants to transfer money to Alice, the transaction is triggered by Bob and is referred as a transaction which is broadcasted to everyone involved within the network. Now the transaction needed to get approval to get valid status by this ecosystem of Blockchain. Once it is approved as valid with its hash then it is fed into a new block of succeeding block, and are communicated with all the nodes that are participating so that it can appended to the Block chain ledger [3].

3. **Terminologies Related to Blockchain:** Now a day's every industry is eagerly trying to adopt Blockchain technology for their business to grow so to better understand this technology we must be familiar with its terminologies. Here are some of them which are more significant.

- **Genesis Block:** This is the first block of a network ok blockchain and is also considered as pioneering record. Moreover, this block comprises of all the rules and configurations that are responsible for running of a Blockchain smoothly. It has an index similar like other data structures and a serial number is assigned to each block and this serial number is termed as block's height.

- **Block:** All the main things in a Blockchain network revolves around the concept of block and block can be considered as the foundation of this technology. Inside the block, every set of data and record is stored that is produced in the network. It acts like a container for holding the data of the Blockchain.

- **Markle Tree:** This is basically a data structure. It stores the data in a unique way as every branch of this tree has its unique identifier and also contains the reference to all other branches connected to it. Hence if someone wants to determine the validity of stored data then it can be simply done by ensuring the leaves should have exact reference points. This tree basically represents all the blocks as in a transaction.

  - **Mining:** Mining can be said as the core of a Blockchain network as it points to the creation of every new block which contains the record. Creation of block is irreversible and cannot be undone.

- **Token:** It is the most basic entity which cannot be further divided to smaller unit. It is mostly a whole number but in case of the crypto-currency it can be a fractional number.

  - **Coin:** Unlike token a coin has its own network of Blockchain. Coin of Ethereum network known as ETH and rest all the things are known as token.

  - **Wallet:** This is basically a vault in which all digital assets are stored. It is an entity which provide security by providing private keys and hence allowing to communicate across the network.

  - **Block Reward:** It is basically a concept used only in the cases of crypto-currency in which a network is allowed to each consensus by rewarding the miners in terms of resources and energy.

  - **Certificate Authority:** It issues digital identities to all the members present on the Blockchain network. A CA is there to validate the ID of the parties involved in the transaction on the network.

- **Turing Complete:** It is simply a term that indicates the technological ability to simulate the turing machine in every aspect.

  - **Blockchain Node:** This is a part of the Blockchain and its work is to connect the network with other peers and also to create new publishing and blocks for every new transaction on the network.

- **Hash Function:** This is a cryptographic function which takes input and gives a encrypted output that is totaly different from the original input. The output cannot be predicted even if the input is same so these functions are very popular in Blockchain technology.

  - **Forks:** When a network is created in case of crypto-currency from the existing network it is reffered as a forks. This newly created network inherits everything from the parent network i.e its architecture and procedures and can be instantiated from parent network.

- **Consortium:** This is a type of abstracted blockchain or we can say private Blockchain and is hided from general public. It is only for fewer members of the organization. A high level access is required to work over such private network.

  - **DApp:** This refers to a decentralized application and therefore it is named so. Since the database is decentralized it can be trusted more for the sake of data security of the end users.

  - **Ethereum Virtual Machine**: Whenever the network has an agreement over a new block the state of the network is updated to a new state so EVM is helpful in achieving this agreement over the network by using e-WASM byte-code to manage transitions. Also it should be known that the state of every node is same and if its different the consensus is not reached and this will lead to the failure of a Blockchain network.

  - **Exchange:** This a platform for the users which s very simple to operate and where the users can trade their digital assets like Bybit, CoinBase etc.

  - **Gas Price:** This is basically a nominal fee taken by the network to complete your transaction by acting as a middleman for the transaction over the network in similar way as bnk charges some amount for every transaction.

  - **Gossip Protocol:** It provide an interface for the users of the Blockchain network to communicate across the network. It is essential to maintain the exact same copies of the ledger.

- **Testnet:** This provides a private protocol for the developers for the purpose of testing before deploying anything for th use of general public over a Blockchain network.

- **Mainnet:** Once the Blockchain is completely developed then the mainnet is used to deploy it so that the complete usage can be done by general public.

- **Merkle Root:** It is point where every branch of the tree meets or we can simply say it has all the hash functions of all the transactions that occurs on the network.

- **Public Key:** This is an identity over a Blockchain network which allows a user to receive funds and to decrypt the received message of the sender.

  - **Private Key:** It is similar to public key but is not known to anyone and this is responsible for encrypting every transaction that a sender will make to send a message over a Blockchain network.

  - **Secure Hash Algorithm:** This is basically an algorithm to generate a secure hash function for every input of the user.

- **Non-Fungible Token:** It is a type of digital currency which cannot be divided into fractions and will always remains as a whole number. These are used for assigning NFT to a file which is making sense as a complete file like a music file.

4. Types of Blockchain

- **Public Blockchain:** This means a Blockchain which is permission-less and not restricted and is distributed as a ledger system. Any end user can access this Blockchain by simply entering credentials and become an authorized member of the network. A user who is a part of Blockchain which is public is allowed to access the current and the past records and can also verify every transactions and mining. The basic use of such Blockchain is for currency exchange and mining. If the security rules and protocoles are followed by the users the public Blockchain is said to be secure and if they dont follow the rules it cant be said as a secure.

- **Private Blockchain:** This type of Blockchain are very restrictive and need permissions to be a part of such network. These are basically used in an enterprise or an organization in which there are only a limited amount of users in the organization for a Blockchain network. The condoling organisation is the in-charge of authorizations, security, permissions, and accessibility levels. As a result, private Blockchains function in a manner similar to public Blockchains although have a smaller, more limited network. Blockchain private networks are used for voting, operating the network of supply, digital identification, ownership of assets, etc. Examples of private blockchain projects includes Multichain and Hyperledger (Fabric, Sawtooth), Corda, and others.

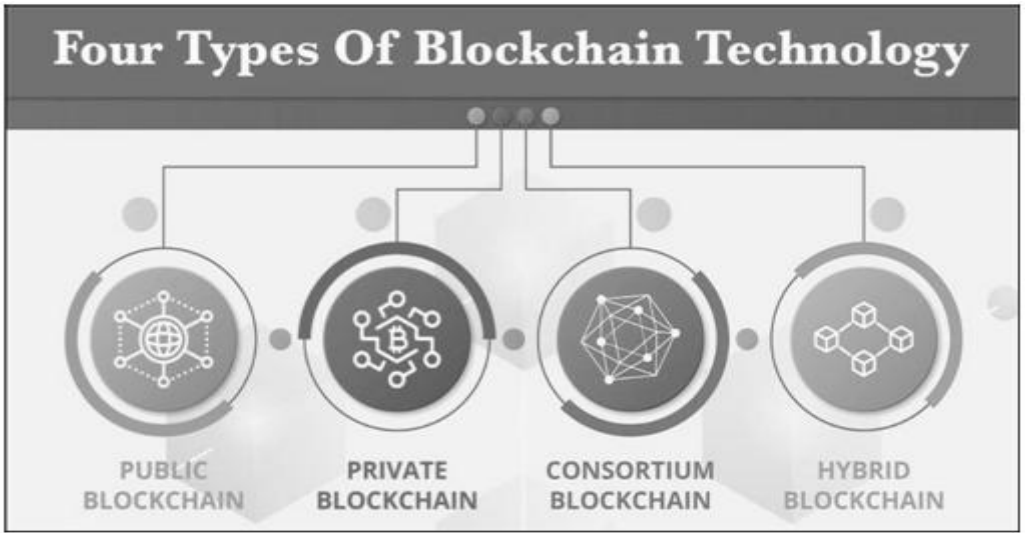

Figure 2: Types of Blockchain

- **Hybrid Blockchain:** A hybrid blockchain is one that combines the features of public and private Blockchains. It makes use of both the private permission-based system and the public permission-less system aspects of Blockchains. Users may manage who has access to what data stored in the Blockchain with the use of such a hybrid

network. Only a certain subset of data or records from the Blockchain may be made public, keeping the remainder secret and confidential. Users may simply link a private Blockchain with many public Blockchains because to the flexibility of the hybrid blockchain technology. A hybrid Blockchain's private network is typically used to verify a transaction. However, users may also publish it on the open Blockchain in order to be confirmed. Public Blockchains involve additional nodes for verification and boost hashing. As a result, the Blockchain network's security and transparency are improved. Dragon chain is an illustration of a hybrid Blockchain.

- **Consortium Blockchain:** A collective Blockchain is a semi-decentralized kind in which a network of Blockchains is managed by many organisations. Opposite to what we saw in a private Blockchain, which is controlled by only one organisation, this is not the case. In this kind of Blockchain, many organisations may function as nodes, exchanging data or engaging in mining. The usual users of consortium blockchains include financial institutions, governmental bodies, etc. Blockchain consortium examples include the Energy Web Foundation, R3, and others.

5. Applications of Blockchain

- **Healthcare:** By enhancing the privacy, security, and interoperability of healthcare data, blockchain can play a significant role in the healthcare industry. It has the potential to alleviate a number of the industry's interoperability issues and enable the safe exchange of healthcare data amongst the numerous parties and individuals engaged in the process. It also minimizes administrative expenses and removes third-party meddling. By using digital signatures and encryption to preserve privacy, healthcare records may be kept in distributed data bases using blockchain technology.

  - **Government:** Blockchain technology has the potential to revolutionise how government functions and provides services. It might be crucial in resolving the data transactional issues facing the government sector, which now operates in silos. [8] Better data management across several departments is made possible by the right connection and sharing of data using Blockchain. It increases openness and offers a more effective approach to keep track of and audit the transactions.

- **CPG and Retail:** Blockchain technology has a tonne of potential applications in the retail industry. This covers a wide range of activities, such as verifying the authenticity of expensive products, stopping fraud, tracking down stolen goods, providing virtual warranties, controlling loyalty programmes, and optimising supply chain processes.

II. LITERATURE SURVEY

The open, distributed blockchain stores records of transactions between two parties. This kind of permanent, verifiable record-keeping is one of the best ways to keep track of transactions. An open-source framework is used to build Blockchains. These Blockchains may be built in a variety of ways to meet the needs of various industries. Every transaction is recorded on several computers since Blockchain is a distributed ledger, removing any

possibility of data loss. Blockchain is dispersed, thus no one entity can completely own or control it. Transactions are conducted without the involvement of third parties, which lowers costs. The only time a transaction may be amended is after it has been completed. A review of current blockchain-related writing is presented in this section. Google Scholar, IEEExplore, and other scholarly search engines were utilized to gather the literature for this chapter. The following keywords were used in searches for the articles: "Blockchain," "Blockchain applications," "Blockchain survey," "Blockchain consensus," "Ethereum," "Ethereum survey," "Uniswap," and "Cryptocurrency." Articles from the years 2008 through 2022 were looked up. We made an effort to be as detailed as we could when it came to posting year and report sources.

The chapter's organisation is as follows: Section-A contains the study on blockchain technology. Section-B discusses the emergence of a wide range of applications in corporate operations that rely on blockchain to offer security, transparency, and protection. Section-C presents a selection of papers on cryptocurrencies, which are virtual currencies designed to be used as a means of exchange across decentralized computer networks. Section-D covers cryptocurrency trading, which comprises buying and reselling digital assets for a profit. Section-E discusses the development of various decentralized Applications outside the purview and control of a single authority. In-depth research on the Uniswap platform, which uses a number of smart contracts to handle transactions on its exchange, is described in Section-F.

1. Blockchain as A Technology

- **The original Bitcoin article by Satoshi Nakamoto: Bitcoin: A peer-to-peer electronic cash system S. Nakamoto, 2008:** The usage of Blockchains as immutable ledgers is the basis of current Blockchain technology. With this paper, the Bitcoin and Blockchain revolution was launched. In spite of the fact that the article was released as a non-peer-reviewed white paper, it is one of the most often cited publications in the subject of Blockchain study. The essay is succinct and doesn't get too specific. It basically covers Bitcoin's basic idea and layout as a cryptocurrency. The report withholds details about the solution, specific technologies, and the particular features and techniques of putting the Bitcoin system into practice. Another interesting fact is that Satoshi Nakamoto avoided mentioning the term "blockchain" in his paper. But he does talk about chain lengths, proof-of-work chains, and block chains. [4].

- **Ethereum White Paper A Next Generation Smart Contract & Decentralized Application Platform By Vitalik Buterin, 2014:** Ethereum aims to combine and improve the ideas of scripting, altcoins, and on-chain meta-protocols in order to allow developers to create arbitrary consensus-based applications that have the scalability, standardization, feature-completeness, ease of development, and interoperability offered by these various paradigms all at the same time. Ethereum does this by developing what may be regarded as the most abstract fundamental layer imaginable: With a built-in Turing-complete programming language, anybody may create smart contracts and decentralized apps on a Blockchain, allowing them to set their own arbitrary rules for ownership, transaction forms, and state transition processes. In its simplest form, Name Coin may be implemented with just two lines of code, while

other protocols, such as currencies and reputation systems, can be developed in less than twenty. Smart contracts, which are cryptographic "boxes" that hold value and only unlock it if certain criteria are satisfied, may also be constructed on top of our platform thanks to the added features of Turing completeness, value-awareness, Blockchain awareness, and state [5]. Compared to those offered by Bitcoin programming, these contracts have a lot more power.

- **Where Is Current Research on Blockchain Technology? A Systematic Review, 2016:** An integrated data management and transaction system called blockchain was first developed for the Bitcoin digital currency. Interest in blockchain has been generated by its key features, which include security, privacy, and integrity without a third-party organisation. Their aim was to comprehend the technological concerns, issues, and potential future directions around Blockchain technology. The majority of research focuses on locating and fixing security and privacy issues with Blockchain [6].

- **Understanding Blockchain Technology Simanta Shekhar Sarmah, 2018:** Blockchain is one of the most significant technological advancements in recent years. Blockchain has transformed trade by establishing a transparent method of monetary exchange. There has been a significant surge in investments from companies and IT behemoths in the Blockchain industry, which is predicted to have a net worth of more than $3 trillion dollars in the next five years. It has grown in popularity as a result of its undoubted security and ability to handle all difficulties associated with digital identity. It is the digital ledger of a peer-to-peer network. This research [7] covers the history, architecture, operating principles, advantages and disadvantages, and several uses of the Blockchain technology.

- **A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities Ahmed Afif Monrat, Olov Schelén, (Member, IEEE), and Karl Andersson, (Senior Member, IEEE), 2019:** A distributed, decentralised database called a blockchain is used to store information using digital signatures. Thanks to the qualities of Blockchain, such as decentralisation, immutability, transparency, and audibility, transactions are more safe and resistant to manipulation. Blockchain technology may be used in industries other than cryptocurrency, such as risk management, healthcare facilities, financial services, and social services. The promise that blockchain technology offers in a variety of application industries is the focus of various academic investigations. In this article, the trade-offs related to blockchain technology were compared. It also contrasted alternative consensus mechanisms, discussed challenges with scalability, privacy, interoperability, energy usage, and legal considerations, and gave an introduction of the taxonomy and architecture of Blockchain [8].

2. Applications of Blockchain

- **Blockchain Technology Applications in Health Care Suveen Angraal, MBBS; Harlan M. Krumholz, MD, SM; Wade L. Schulz, MD, PhD, 2017:** Blockchain technology has experienced a sharp increase in interest recently across a variety of

businesses, including the healthcare industry. Blockchain provides a safe, decentralized database that may operate independently of a manager or central authority. In order to construct a digital ledger on a distributed, peer-to-peer network, blockchain develops a growing, continuous list of ordered information, known as blocks. The network automatically verifies each block of transactions that has been cryptographically signed. Moreover, there is significant interest in blockchain as a platform to improve the veracity and transparency of healthcare data through a range of use cases, such as maintaining access rights in electronic health records (EHR) and accelerating claims processing. The principles of blockchain technology have been defined by the authors of this article [9].

- **Banking on Blockchain: Costs Savings Thanks to Blockchain Technology, 2017:** Blockchain technology has the promise of enhancing the global financial system and enabling more efficient and long-lasting growth than is now achievable. In reality, many organisations are actively focusing on Blockchain technology in order to promote economic growth and speed the development of green technologies. This study looked at the possibilities and challenges of using Blockchain technology to the financial sector, providing some food for thought on the potential of this ground-breaking technology. In order to better comprehend the potential of Blockchain technology to support the financial system, writers looked at the actual functioning of the Bitcoin system while highlighting some of its key disadvantages, such as the high cost of hardware and large energy usage [10].

- **Opportunities and Risks of Blockchain Technologies in Payments– a research agenda, 2017:** The authors recommended three key topics for research. Organizational issues, issues with the competitive environment, and issues with technology design. By examining numerous major themes within each of these areas and developing a series of research questions for each article, we highlight the importance to address risks and opportunities for users and other stakeholder organisations [11].

- **Blockchain Technology: Implications for Operations and supply chain management, 2019:** The authors' objectives in producing this paper were to further the study of Blockchain technology from the perspective of Operations and Supply Chain Management (OSCM), identify potential application domains, and outline a future research agenda. A description and analysis of Blockchain technology were provided in order to ascertain the effects on OSCM [12].

- **A Comparative Study: Blockchain Technology Utilization Benefits, Challenges, and Functionalities, 2021:** Users may confirm, secure, and synchronize the data on a data sheet (a transaction ledger) that is replicated by a number of users by using blockchain technology. It has provided the sector with substantial advantages and incentives to enable for better services. This study looks at the benefits, challenges, and characteristics that affect blockchain implementations across several sectors. Benefits, difficulties, and functions were the three main criteria used to classify the 168 final papers that were selected from a thorough examination of 1976 publications. These papers were produced by organisations in the manufacturing, financial,

governmental, and healthcare sectors. Three dimensions of factors—functionalities (point-to-point transmission, data ownership, data protection, and transaction processing), challenges (technical, organizational, adoption, operational, and environmental and sustainability), and benefits (informational, technological, economic, organizational, and strategic)—were used to extract and compare the results [13].

- **Integrating Blockchain Technology With Internet Of ThingsTo Efficiency, 2021:** The writers' major issue was how to combine Blockchain technology with the Internet of Things. Research must be done in order to improve accuracy, accountability, and confidence among the many parties involved in Blockchain transactions. Improvements to the blockchain architecture and IoT system are required, according to the report. It highlights the need to develop a new model in order to improve efficiency and accuracy. According to this research report, using a decentralized strategy would boost the usefulness of merging Blockchain technology with IoT [14].

3. Cryptocurrency as A Digital Currency

- **An Analysis of the Cryptocurrency Industry Ryan Farell University of Pennsylvania, 2015:** Blockchain, which is managed by "miners," maintains account of all individual transactions and ownership of all crypto-currencies now in use. The usage of Blockchains as immutable ledgers is the cornerstone of today's Blockchain technology. This article provides a concise yet comprehensive introduction of the cryptocurrency industry, concentrating on the first decentralized cryptocurrency, Bitcoin [15].

- **Cryptocurrency, Monia Milinkovic, Faculty of Economics, 2018:** The "digital revolution," which is currently at its height, refers to the shift from analogue and electrical to digital technology. Cryptocurrency is a digital type of money that must exist since we live in an electronic world. Cryptography is a mechanism for making cryptocurrencies, a sort of digital currency, function. Using cryptography, legible data is converted into indecipherable codes. The cornerstone of bitcoin is the digitalized so-called. The term blockchain refers to the primary record of all cryptocurrency watch transactions. Blockchain "miners," who are in charge of updating all transactions that have occurred and guaranteeing the accuracy of the data, are in charge of maintaining Blockchain, which keeps track of individual transactions and ownership of all cryptocurrencies in circulation. This method verifies the transaction's security. This article will discuss cryptocurrencies and their role to economic progress. Cryptocurrency kinds and their evolution in transitional economies will also be highlighted.

- **Multiscale Characteristics of the emerging global cryptocurrency market, 2021:** The authors explained Blockchain technology while discussing the evolution of cryptocurrencies. It has been proved several times that there are distinctions between cryptocurrencies and the exchanges where they are traded. The major component of this study looks at the changes in bitcoin values across several marketplaces.

4. Crypto Trading

- **Preliminary findings on cryptocurrency trading among regular gamblers: A new risk for problem gambling, Devin J. Mills, Lia Nower, 2019:** According to the present data, cryptocurrency trading may appeal to gamblers who have more severe problem gambling. Future research should incorporate cryptocurrency trading into screening, evaluation, and treatment approaches, particularly for gamblers who often engage in it [16].

- **Cryptocurrency Trading Using Machine Learning, Thomas E. Koker and Dimitrios Koutmos, 2020:** The authors suggested an active trading model based on reinforcement machine learning and applied it to five of the most prominent cryptocurrencies currently in circulation. They demonstrated how a buy-and-hold strategy improves risk-adjusted returns while lowering downside risk [17].

- **The psychology of cryptocurrency trading: Risk and protective factors Paul Delfabbro1, Daniel L. King and Jennifer Williams, 2021:** The focus of this study is on investigating possible defensive and instructional measures to protect rookie investors from potential harm as the new activity, most likely investing in bitcoin or stocks, expands and draws a greater number of retail or community investors. The author emphasizes the significance of putting in place safeguards to keep novice investors from making rash or dangerous decisions that might result in financial losses. Furthermore, the report suggests that more specialized research be conducted on the psychological effects of routine trading, individual differences among investors, and the decision-making processes involved in investing. Understanding how regular trading affects individuals psychologically, while taking their specific traits into consideration, might aid in the development of solutions that protect people from unfavorable outcomes while enabling them to capitalize on advancements in blockchain technology [18].

- **Cryptocurrency trading: a comprehensive survey Fan Fang, Carmine Ventre, Michail Basios, Leslie Kanthan , David Martinez-Rego, Fan Wu and Lingbo Li, 2022:** The authors of this paper provide a thorough survey of the field by reviewing 146 research papers on various aspects of cryptocurrency trading (such as cryptocurrency trading systems, bubbles, extreme conditions, prediction of volatility and return, portfolio construction and crypto-assets, technical trading, and others). Furthermore, this study investigates datasets, research trends, and the distribution of research objects (contents/properties) and technologies before concluding with projected cryptocurrency trading alternatives [19].

5. Decentralized Applications

- **The Blockchain-Empowered Software System Wei Cai, (Member, IEEE), Zehua Wang, (Member, IEEE), Jason B. Ernst, (Member, IEEE), Zhen Hong, (Student Member, IEEE), Chen Feng, (Member, IEEE), and Victor C. M. Leung , (Fellow, IEEE), 2018:** In order to demonstrate the significance of decentralised

applications (dApps) and the potential utility of Blockchain, the authors of this study followed the evolution of Blockchain systems [20].

- **A First Look at Blockchain-based Decentralized Applications Kaidong Wu, Yun Ma, Gang Huang, Xuanzhe Liu Key Lab of High-Confidence Software Technology, 2019:** Based on a large dataset of 995 Ethereum DApps and 29,846,075 transaction logs over them, the authors of this paper presented the first thorough empirical study of Blockchain-based DApps to date and then proposed some implications for DApp users to choose appropriate DApps, for DApp developers to improve the efficiency of DApps, and for Blockchain vendors to enhance the support of DApps [21].

- **Distributed Ledger Technology Review and Decentralized Applications Development Guidelines Claudia Antal, Tudor Cioara, Ionut Anghel, Marcel Antal, and Ioan Salomie, 2021:** The authors of this paper offered a thorough review of DLT, analysing the difficulties, offering remedies or alternatives, and discussing how to use them to create decentralised applications. To methodically categorise the technological solutions mentioned in more than 100 articles and startup ventures, they created a three-tier based architecture for DLT applications [22].

III. PROPOSED MODEL

1. **Introduction to Wishper:** By The introduction to Wishper sets the stage for the research, providing a concise overview of the decentralized voting application and its reliance on blockchain technology. Wishper is a cutting-edge platform designed to address the challenges and limitations of traditional voting systems. By leveraging the power of blockchain, Wishper aims to deliver a secure, transparent, and efficient voting experience. In today's world, trust and transparency in voting processes are of paramount importance. Wishper recognizes the inherent flaws and vulnerabilities present in centralized voting systems and seeks to overcome them through the application of blockchain technology. Blockchain, as a decentralized and immutable ledger, offers a unique solution for ensuring the integrity and transparency of voting records. The primary objective of this research is to explore and evaluate the functionality, development process, and technical aspects of Wishper. By doing so, we aim to shed light on the potential impact and advantages of utilizing blockchain technology in the context of voting applications [23]. The research will delve into the core features and functionalities of Wishper, emphasizing its ability to securely record and store voting records on the blockchain. Wishper's decentralized nature ensures that votes cannot be altered or tampered with, fostering trust among participants. Additionally, the application enables transparent auditing of the entire voting process, allowing stakeholders to independently verify the accuracy and fairness of the results. The research will also focus on the development process of Wishper, examining the technologies and tools employed [24]. In particular, the front-end development of Wishper utilizes React.js, a popular JavaScript library known for its flexibility and robustness in creating user interfaces. The

use of React.js ensures a user-friendly and intuitive voting interface, enhancing the overall user experience. Furthermore, the research will explore the requirements and analysis phase of the project. This phase involves gathering and analyzing the functional and non-functional requirements of Wishper. By identifying and validating these requirements, the research team ensures that the resulting application meets the needs and expectations of its users.

2. **Functionality of Wishper:** Wishper is a decentralized voting application that leverages the power of blockchain technology to provide a secure and transparent platform for conducting voting processes. The application offers a range of functionalities that ensure the integrity of the voting system and empower users to participate in democratic processes with confidence [25]. One of the key features of Wishper is its ability to guarantee the immutability of voting records. By utilizing blockchain technology, every vote cast on Wishper is recorded on a distributed ledger that cannot be altered or tampered with. This feature eliminates concerns of fraudulent activities and ensures the accuracy and integrity of the voting process.

   Transparency is another fundamental aspect of Wishper's functionality. The blockchain-based infrastructure enables transparent auditing of the entire voting process. Each vote cast on the platform is visible to all participants, allowing for independent verification of the results. This transparency fosters trust and confidence in the system, as users can personally verify the fairness and accuracy of the voting outcomes [26]. Wishper also provides a secure login process through MetaMask, a popular browser extension that serves as a digital wallet for managing Ethereum-based assets. This integration ensures that each user's identity is authenticated and their voting privileges are properly managed. By requiring users to log in through MetaMask, Wishper prevents unauthorized access and maintains the integrity of the voting process [27].

   The application offers users the opportunity to participate in various voting events and elections. Users can cast their votes on different topics or candidates, expressing their opinions and contributing to the decision-making process. Wishper provides an intuitive and user-friendly interface that enables voters to navigate through the application seamlessly and cast their votes effortlessly. The functionality of Wishper extends beyond the voting process itself. The application allows users to view and track their voting history, providing a transparent and auditable record of their participation. This feature enhances user engagement and encourages continued participation in future voting events [28].

3. **Development of Wishper:** The development of Wishper involved a systematic process that incorporated various technologies and tools to create a robust and efficient decentralized voting application. The project's development phase focused on ensuring the security, transparency, and usability of the platform. To build the front-end of Wishper, React.js was chosen as the primary framework. React.js is renowned for its component-based architecture, which facilitates the creation of reusable and modular UI components. This approach allowed for efficient development, easy maintenance, and

enhanced user experience [29]. HTML and CSS were utilized to structure and style the application, ensuring a visually appealing and intuitive interface. The development team followed an agile methodology, enabling iterative development and frequent feedback loops. This approach allowed for flexibility in adapting to evolving requirements and ensured that the application met the desired objectives.

Throughout the development process, continuous integration and deployment practices were implemented to ensure a smooth and efficient workflow [30]. This involved leveraging tools such as Git for version control and automated testing frameworks to maintain code quality and reliability. Collaboration among team members was facilitated through project management tools, enabling effective communication, task tracking, and progress monitoring. Regular meetings and code reviews were conducted to ensure code consistency, adherence to best practices, and to address any technical challenges [31]. By employing a comprehensive and structured development approach, Wishper was able to meet the functional and non-functional requirements of a secure and transparent voting application. The result is an intuitive and user-friendly platform that leverages blockchain technology to provide a trustworthy voting experience [32].

4. **Frontend of Wishper:** The frontend development of Wishper plays a crucial role in providing users with an intuitive and engaging voting interface. The chosen technologies for frontend development are React.js, HTML, and CSS, which collectively contribute to the creation of a visually appealing and user-friendly application. React.js, a JavaScript library, serves as the foundation for building the frontend of Wishper [33]. It employs a component-based architecture, allowing developers to break down the user interface into reusable and modular components. This approach simplifies the development process, enhances code reusability, and improves maintainability. HTML (Hypertext Markup Language) is used to structure the content of the application [34]. It provides a standardized markup language that defines the layout and organization of elements on web pages. With HTML, the research team can define the structure of the voting interface, including buttons, forms, input fields, and other interactive element [35].

   CSS (Cascading Style Sheets) is utilized to add styling and visual enhancements to the application. It enables the research team to define colors, fonts, spacing, and other presentational aspects of Wishper's user interface. CSS ensures consistency in design across different screens and devices, creating a seamless and cohesive user experience [36].

   By leveraging React.js, HTML, and CSS, the frontend development team can create a responsive and interactive voting interface for Wishper. The component-based approach of React.js enhances code maintainability and reusability, while HTML and CSS provide the necessary structure and styling to make the interface visually appealing and user-friendly. The combination of these technologies enables users to navigate the application effortlessly, cast their votes, and engage in the voting process with ease [37] [38].

IV. USER INTERFACE AND RESULT

1. Our User Interface

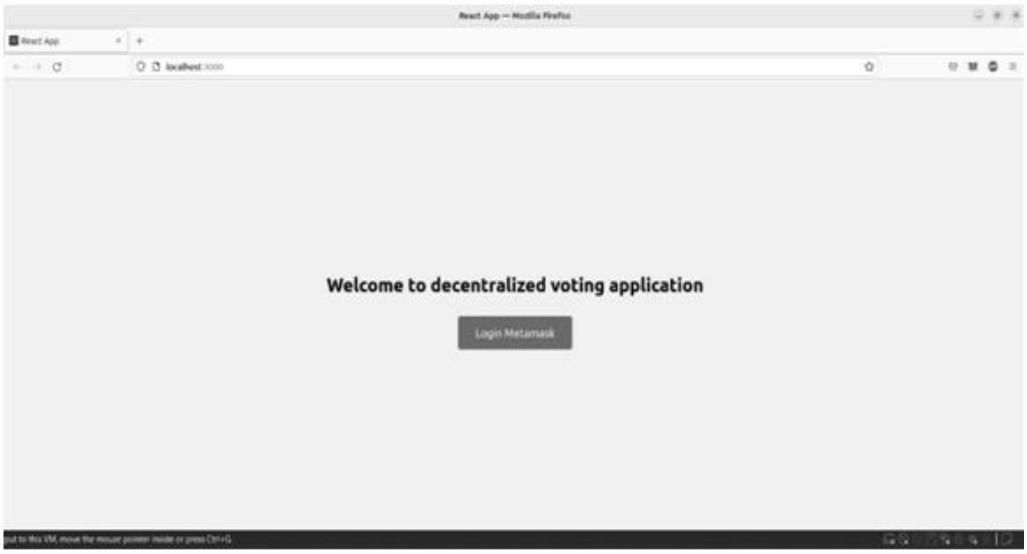

Figure 3: User Interface

2. Connecting Wallet

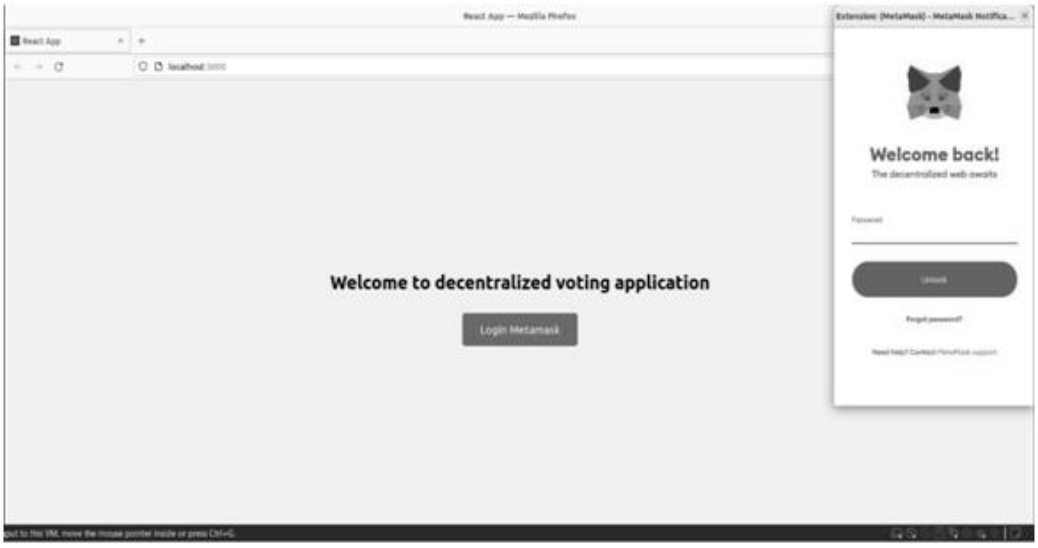

Figure 4: Connecting Wallet

3. Connected

Figure 5: Connected

4. Voting

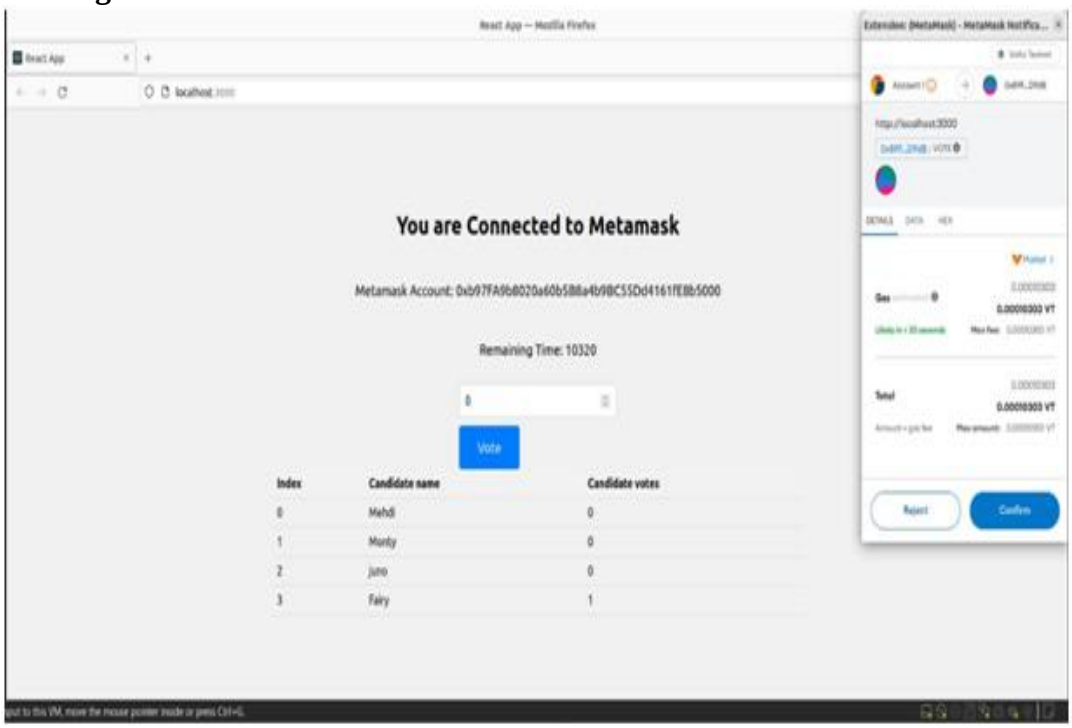

Figure 6: Voting

5. Voted

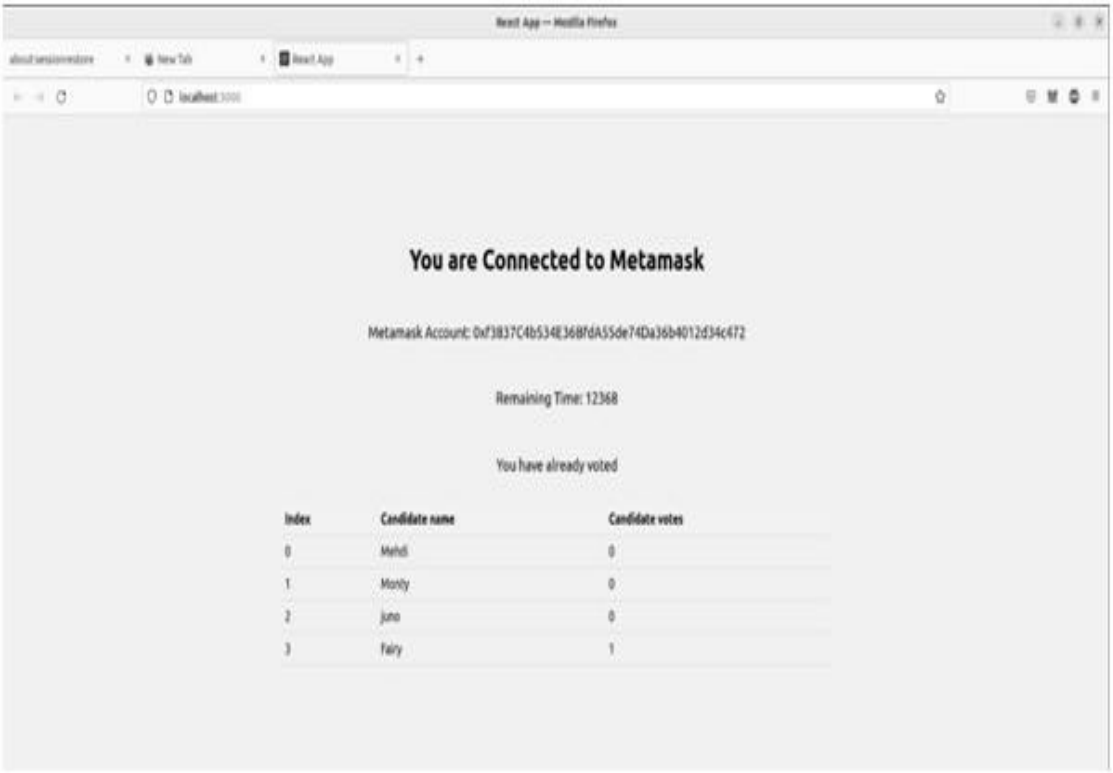

Figure 7: Voted

6. Waiting for Time to Complete

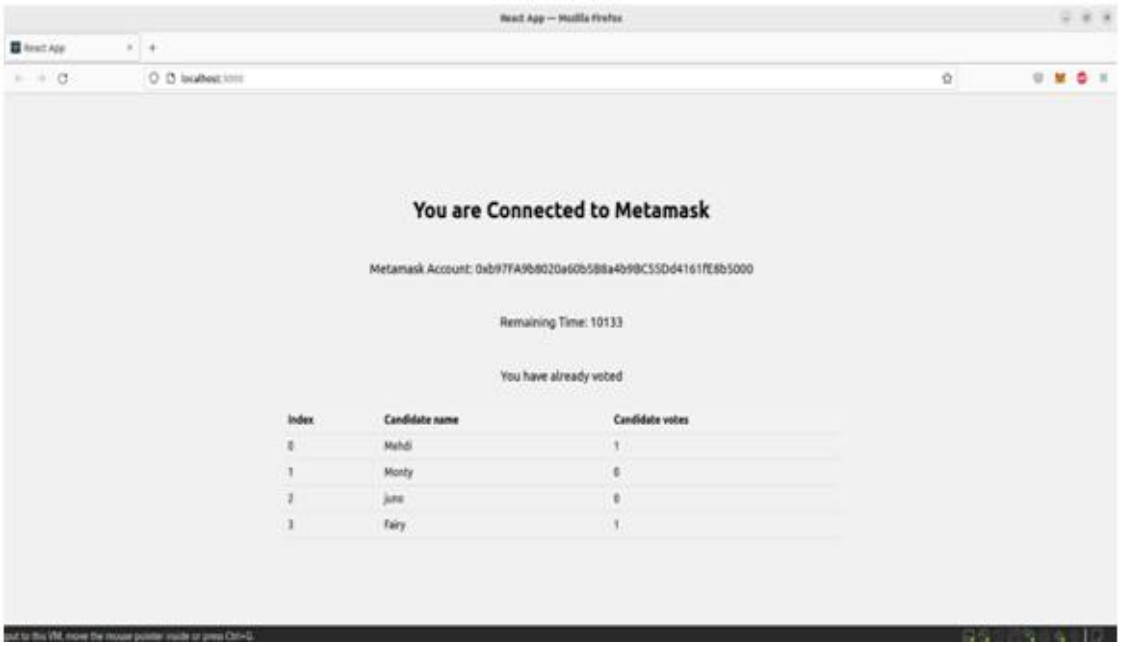

Figure 8: Waiting for Time to Complete

7. Voting Finished

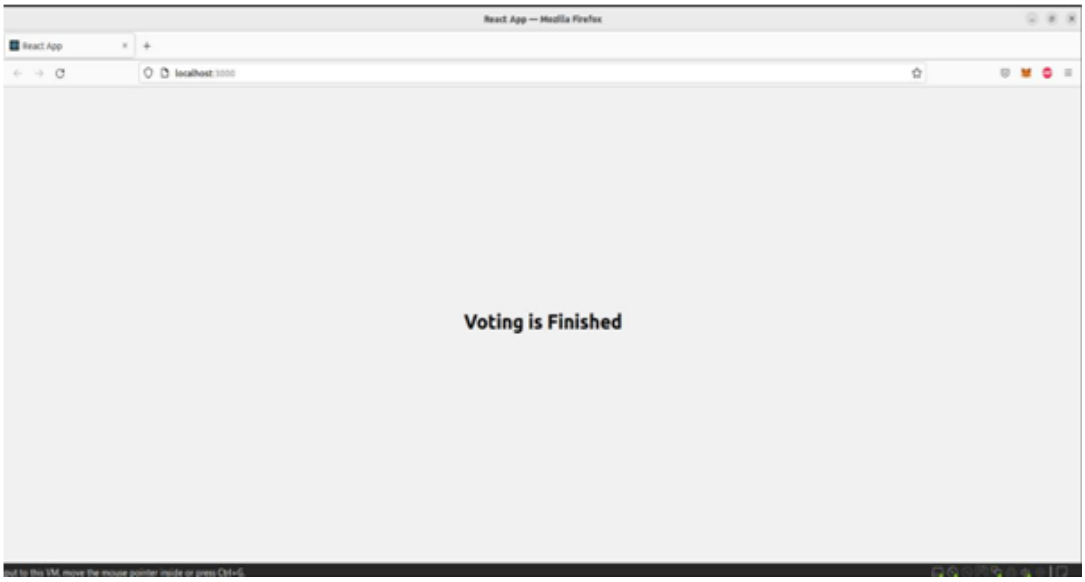

Figure 9: Voting Finished

V. CONCLUSION AND FUTURE SCOPE

CONCLUSION

Despite Blockchain-based digital assets being traded since 2009, a functional gap exists between on-chain transactions and trust-based centralized exchanges. This was bridged with the success of Uniswap, a decentralized exchange whose constant product automated market enabled the trading of Blockchain tokens without relying on market makers, bids, or asks. It provided us with a new decentralized financial system. The current work presented a demonstration of a Dex where people can swap crypto-tokens using goerli test Ethereum.

We are developing this project to demonstrate platforms like Uniswap to our country, where everyone can't buy and exchange cryptocurrencies, and this will also explain and make people aware of this technology. This real-time solution targets users prioritizing security, hustle-free, and economic applications for cryptocurrency engagements. The application makes them aware of the Fintech solutions which will rule the coming era, consequently increasing their belief in Blockchain-based solutions.

The Wishper platform aims to enable users to trade cryptocurrencies without the involvement of a centralized third party in a secure manner. The overall aim of prioritizing security, hustle-free, and economic cryptocurrency engagements to enable users to trade cryptocurrencies without the involvement of a centralized third party in a secure manner is duly fulfilled by our application.

FUTURE SCOPE

In future, looking forward on large scale distribution of our project along with involvement of investment we will add functionalities like providing access to other cryptocurrencies for swapping as well as we'll deploy our contract on Ethereum main net network to allow users to trade cryptocurrencies without an involvement of a centralized third party in a secure manner.

1. **Future Applications**: Wishper, the decentralized voting application, has the potential to revolutionize major elections, setting new standards of inclusivity, security, and efficiency. By incorporating a person's identity card or ID number and linking it to their MetaMask account, Wishper enables individuals to exercise their voting rights conveniently and securely from anywhere in the world. This groundbreaking approach paves the way for a future where democratic processes are enhanced and electoral participation is maximized.

2. **Advantages of Wishper**

- **Unprecedented Accessibility:** Wishper's remote voting capability eliminates barriers posed by geographical constraints, physical disabilities, or time limitations. By enabling individuals to cast their votes from any location with an internet connection, Wishper ensures that every eligible voter has the opportunity to participate actively in major elections.

- **Robust Security and Transparency:** Through the utilization of blockchain technology, Wishper guarantees the highest level of security and transparency in the voting process. The immutability of the blockchain ensures that voting records remain tamper-proof, creating an environment where every vote is accurately recorded and preserved. This instills confidence in both voters and electoral authorities, fostering trust in the integrity of major elections.

- **Streamlined Verification and Authentication:** By integrating a person's identity card or ID number and leveraging MetaMask for authentication, Wishper simplifies the verification and authorization process. Each individual's identity is securely linked to their MetaMask account, ensuring a seamless and trustworthy voting experience. This streamlined approach enhances the efficiency of the electoral process, enabling quick and reliable verification of voter eligibility.

- **Prevention** of Electoral Fraud: Wishper's implementation of unique identification, such as a roll number or election card number, coupled with the use of MetaMask, guarantees that each individual can cast only one vote. This robust safeguard eliminates the possibility of duplicate voting or fraudulent activities, reinforcing the fairness and credibility of major elections.

- **Tokenized Voting System for Enhanced Accountability**: Wishper leverages the power of blockchain-based tokens, such as non-fungible tokens (NFTs), to create an auditable and transparent voting system. By issuing unique tokens to authorized

voters in their connected MetaMask accounts, Wishper ensures that each vote can be traced back to its origin, enhancing accountability and eliminating doubts about the integrity of the electoral process.

REFERENCES

[1] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. PLoS ONE, 11(10), e0163477. doi: 10.1371/journal.pone.0163477.

[2] Garg, K., Gupta, A., Nirwal, A., & Kumar, R. (2022). What and Why You Need to Know about Non-Fungible Tokens (NFTs). International Journal of Scientific Research in Engineering and Management (IJSREM), 06(06), 1-7. ISSN: 2582-3930.

[3] Kumar, R., Soni, P., Aggarwal, A., Kumar, M., Mishra, N. (2022). An Analytical Approach for Sustainable Development in Smart Society 5.0 Using Swasthya Sahayak Application. In: Bali, V., Bhatnagar, V., Lu, J., Banerjee, K. (eds) Decision Analytics for Sustainable Development in Smart Society 5.0. Asset Analytics. Springer, Singapore. https://doi.org/10.1007/978-981-19-1689-2_9

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] Vitalik Buterin, "Ethereum White Paper A Next Generation Smart Contract & Decentralized Application Platform," 2014.

[6] Jesse Yli-Huumo, "Where Is Current Research on Blockchain Technology? A Systematic Review," 2016.

[7] Simanta Shekhar Sarmah, "Understanding Blockchain Technology," 2018.

[8] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson, "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities," 2019.

[9] Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology: Applications in Health Care. Circulation: Cardiovascular Quality and Outcomes, 10. doi:10.1161/CIRCOUTCOMES.117.003800

[10] Cocco L, Pinna A, Marchesi M. Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology. *Future Internet*. 2017; 9(3):25. https://doi.org/10.3390/fi9030025

[11] Lindman, J., Tuunainen, V. K., & Rossi, M. (2017). Opportunities and Risks of Blockchain Technologies – A Research Agenda. In Proceedings of the 50th Hawaii International Conference on System Sciences (pp. 1-10).

[12] Cole, R., Stevenson, M., & Aitken, J. (2019). [Blockchain technology: implications for operations and supply chain management - 2019]. Supply Chain Management, 24(4), 469-483. doi:10.1108/SCM-09-2018-0309

[13] O. Ali, A. Jaradat, A. Kulakli and A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," in *IEEE Access*, vol. 9, pp. 12730-12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[14] Alsharari, N. (2021). Integrating Blockchain Technology with Internet of things to Efficiency . International Journal of Technology, Innovation and Management (IJTIM), 1(2), 01–13. https://doi.org/10.54489/ijtim.v1i2.25

[15] Farell, R. (2015). An Analysis of the Cryptocurrency Industry.

[16] Mills, D. J., & Nower, L. (2019). Preliminary findings on cryptocurrency trading among regular gamblers: A new risk for problem gambling? Addictive Behaviors, 92, 136-140. ISSN 0306-4603. https://doi.org/10.1016/j.addbeh.2019.01.005

[17] Koker, Thomas E., and Dimitrios Koutmos. 2020. "Cryptocurrency Trading Using Machine Learning" *Journal of Risk and Financial Management* 13, no. 8: 178. https://doi.org/10.3390/jrfm13080178.

[18] Delfabbro P, King DL, Williams J. The psychology of cryptocurrency trading: Risk and protective factors. J Behav Addict. 2021 Jun 19;10(2):201-207. doi: 10.1556/2006.2021.00037. PMID: 34152998; PMCID: PMC8996802.

[19] Fan Fang & Carmine Ventre & Michail Basios & Leslie Kanthan & David Martinez-Rego & Fan Wu & Lingbo Li, 2022. "Cryptocurrency trading: a comprehensive survey," Financial Innovation, Springer;Southwestern University of Finance and Economics, vol. 8(1), pages 1-59, December.

[20] Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized Applications: The Blockchain-Empowered Software System. IEEE Transactions on Services Computing, 11(3), 446-458.

[21] Wu, Kaidong & Ma, Yun & Huang, Gang & Liu, Xuanzhe. (2019). A First Look at Blockchain-based Decentralized Applications.
[22] Antal C, Cioara T, Anghel I, Antal M, Salomie I. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet*. 2021; 13(3):62. https://doi.org/10.3390/fi13030062
[23] Rajender Kumar, Vipin Tomar, Punit Soni, & Satveer Kour. (2023). Implementing Data-driven Approach for Institutional Decision-making in Higher Education. International Journal of Wireless & Mobile Networks (IJWMN), 01(01), 01-06.
[24] Kumar, R., Khanna, R., & Kumar, S. (2022). Technological Transformation of Middleware and Heuristic Approaches for Intelligent Transport System. *Autonomous Vehicles Volume 1: Using Machine Intelligence*, 61-82.
[25] Gaba, S., Nagpal, S., Aggarwal, A., Kumar, R., & Kumar, S. (2022, November). An Analysis of Internet of Things (IoT) Malwares and detection based on Static and Dynamic Techniques. In *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 24-29). IEEE.
[26] Chatha, D., Aggarwal, A., & Kumar, R. (2022). Comparative Analysis of Proposed Artificial Neural Network (ANN) Algorithm With Other Techniques. In *Research Anthology on Artificial Neural Network Applications* (pp. 1218-1223). IGI Global.
[27] Kumar, R., Khanna, R., & Kumar, S. (2021). Vehicular middleware and heuristic approaches for intelligent transportation system of smart cities. In *Cognitive Computing for Human-Robot Interaction* (pp. 163-175). Academic Press.
[28] Kumar, R., Khanna, R., & Kumar, S. (2018). Deep learning Integrated approach for collision avoidance in Internet of Things based smart vehicular networks. Journal of Advanced Research in Dynamical and Control Systems, 10(14), 1508-1512.
[29] Kumar, R., Khanna, R., & Kumar, S. (2018). An effective framework for security and performance in Intelligent Vehicular ad-hoc network. *Journal of Advanced Research in Dynamical and Control System*, *10*(14), 1504-1507.
[30] Kumar, R., & Kumar, R. (2016). A Comparative Analysis of Performance Metrics of Different Cloud Scheduling Techniques. International Journal of Innovations in Engineering & Technology, 7(2), 222-226. ISSN: 2319-1058.
[31] Sardana, S., & Kumar, R. (2016). Energy Efficient Target Tracking in Wireless Sensor Networks. International Journal of Innovations in Engineering & Technology, 7(2), 271-275. ISSN: 2319-1058.
[32] Gupta, G., & Kumar, R. (2016). Acoustic Channel Modeling and Simulation for Underwater Acoustic Wireless Sensing Networks. *International Journal of Computer Applications*, *975*, 8887.
[33] Kumar, R., Khanna, R., & Verma, P. K. (2014). Middleware Architecture of VASNET and Its Review for Urban Monitoring & Vehicle Tracking. International Journal of Emerging Research in Management & Technology, 3(1), 41-45.
[34] Garg, T., Kumar, R., & Singh, J. (2013). A way to cloud computing basic to multitenant environment. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(6), 2394-2399.
[35] Kumar, R., Khanna, R., & Kumar, S. (2013). A Proposed work on Node Clustering & Object Tracking Processes of BFOA in WSN. International Journal of Computer Science & Communication, 4(2), 207-212.
[36] R. Kumar , R. Khanna , S. Jangra , and P. K. Verma , " A study of diverse wireless networks ," IOSR Journal of Engineering , vol. 2 , no. 11 , pp. 01 – 05 , 2012 .
[37] Kumar, R., Verma, P. K., & Verma, P. K. (2012). Role of Information Communication Technology and its Impact on Health Sector. ijarcs, 1(2), 122-125.
[38] Kumar, R., & Batra, A. (2011). Employing Grid Comparative Strategies in Cloud Computing. IJCSIT-ISSN 0975-9646, 2(5), 2246-2253.

