Blockchain-Based Voting Systems: Revolutionizing Democratic Processes for Secure, Efficient, and Transparent Elections

Mehdi
B.Tech Scholar,
Department of IT

Vipin Tomar
Assistant Professor,
Department of CSE

Rajender Kumar
Associate Professor,
Department of CSE

[123]Panipat Institute of Engineering and Technology, Samalkha, Panipat, India

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, blockchain technology ensures the integrity and transparency 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

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 such as Bitcoin, but its potential applications extend far beyond the realm of digital money. A blockchain is essentially a series of blocks, each of which contains a list of transactions or data. These blocks are linked together with cryptographic hashes to form an immutable and tamper-resistant chain. Once a transaction or piece of data is 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].

A. **Blockchain**

The Blockchain is an encrypted, distributed database that records data, or in other words it is a digital ledger of any transactions, contracts - that needs to be independently recorded. One of the key features of

Blockchain is that this digital ledger is accessible across several hundreds and thousands of computer and is not bound to be kept in a single place. Blockchain chain has already started disrupting the financial services sector, and it is this technology which underpins the digital currency- bitcoin transaction. Blockchain is an open and distributed ledger that can be used to record transactions between two parties. This way of recording a transaction is both permanent as well as verifiable, which makes it one of the best ways to keep transactions. Blockchains are built on the open-source platform. So different versions of these Blockchains are possible, which are developed as per the needs of different industries [2].

B. **Working of Blockchain**

For a new transaction to be added to the existing chain, it has to be validated by all the participants of the relevant Blockchain eco-system. For such a validation and verification process, the participants must apply a specific algorithm. The relevant Blockchain eco-system defines what is perceived as "valid", which may vary from one ecosystem to another. A number of transactions, thus approved by the validation and verification process, are bundled together in a block. The newly prepared block is then communicated to all other participating nodes to be appended to the existing chain of blocks. Each succeeding block comprises a hash, a unique digital fingerprint, of the preceding one.

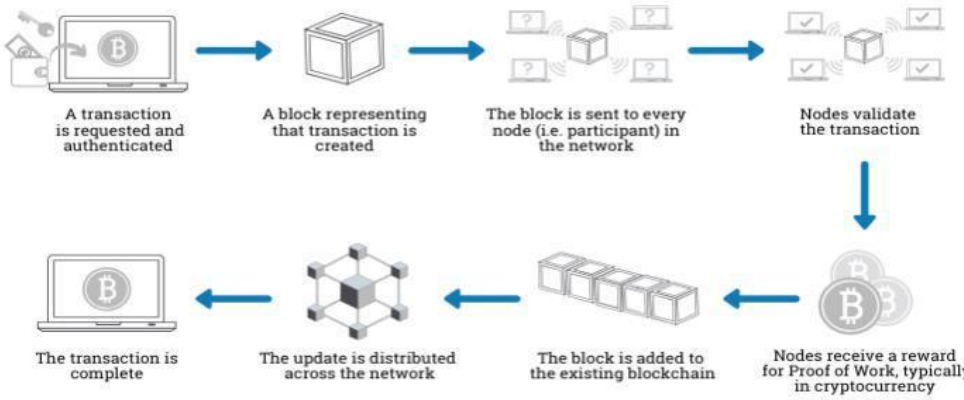

Figure 1: Blockchain transaction.

Figure 1 demonstrates how Blockchain transactions takes place, using a step by-step example. Bob is going to transfer some money to Alice. Once the monetary transaction is initiated and hence triggered by Bob, it is represented as a "transaction" and broadcast to all the involved parties in the network. The transaction now has to get "approval" as being indeed "valid" by the Blockchain eco-system. Transaction(s) once approved as valid along with the hash of the succeeding block are then fed into a new "block" and communicated to all the participating nodes to be subsequently appended to the existing chain of blocks in the Blockchain digital ledger [3].

C. **Terminologies related to Blockchain**

Since Blockchain technology is experiencing a significant boom and every second industry is eager to adopt it in various use cases, it is required for you, as an internet user, to know about some essential terminologies in this regard.

- **Genesis Block:** It happens to be the very first block on a Blockchain network and can also be considered as the pioneering record. Apart from this major distinction, this block is also different from the rest of the blocks as it mainly contains the configurations and rules for the smooth running of the Blockchain. Just like any other data structure, there is an index or rather a "serial number" assigned to each block, which in this context is referred to as the block's height and its relative to the genesis block.

- **Block:** Everything in the Blockchain sphere revolves around the concept of blocks. In fact, it's the foundation of this technology. Every record or data that the network produces is essentially stored inside a block and every time a record is created, there is a new block to contain it. In other words, you can also think of it as a container for holding the Blockchain data.

- **Markle Tree:** It is rather a technical concept as it's a data structure. Although it contains the data, the way it stores it is quite unique because each branch of the tree has an identifier and contains references to all the

subsequent branches attached to it. Therefore, instead of going through the entire data set, anyone can determine the validity of the stored data on different nodes by ensuring that the leaves contain the same reference points. If we view it particularly from the Blockchain's perspective, the branches of a merk-le tree represent blocks in a transaction.

- **Mining:** This is the core of any Blockchain network and refers to the creation of a new block creation of a new block that contains the record. Once a block is created, there is no reversal for this operation.

- **Token:** If you have traded crypto-currencies, you already know that it's possible to buy them in fractional amounts as well, unlike fiat. Therefore, by that analogy, a token is the most basic unit of a crypto-currency that cannot be further divided. In fiat, it's always a whole number but in crypto-currencies, it is mostly a fractional number. Another major distinction is that tokens do not have their own Blockchain and in fact, a project that offers tokens, runs on a Blockchain provided by 3rd party.

- **Coin:** From a layman's point of view, there is no distinction between a coin or a token. However, from the technical perspective, it is worth noting that a coin has its own Blockchain network. To put it straight and make it easier to understand, ETH is the coin of the Ethereum network but all other projects or crypto-currencies on this network are tokens.

- **Wallet:** It happens to be a "vault" where digital assets (i.e. crypto-currencies) are stored. But from a technical standpoint, a wallet is a secure entity that contains an individual's private keys , allowing him to communicate on the network and sign transactions.

- **Block Reward:** This term is only valid for cryptocurrency use cases where miners are essentially rewarded for the resources and energy they spend for mining and allowing the network to reach a consensus.

- **Certificate Authority:** This is an entity on a Blockchain network that issues digital identities to all members. Moreover, every time a transaction is to be signed, the CA is responsible for validating the IDs of the involved parties.

- **Turing Complete:** This is a term commonly used in the Blockchain industry and quantum computing as well and it refers to the ability of technology to simulate the Turing machine in all aspects.

- **Blockchain Node:** It is a member of a Blockchain network that is connected to several other peers and is responsible for creating new blocks and publishing new transactions on the network.

- **Hash Function:** It happens to be a cryptographic function that takes an input and changes the output entirely (this new output is used to represent the original information). The reason why it's so popular among Blockchain enthusiasts is that the output of hash functions can never be predicted.

- **Forks:** This concept is native to crypto-currencies and it refers to an event where a new network is created from an existing one. In most cases, the new network inherits the consensus and architecture of its predecessor and can even instantiate itself from the original network. One of the primary reasons for conducting a fork is when the network fails to reach a consensus on most of its core decisions. That is when the developers decide to create a separate Blockchain network and introduce their ideas, which again need to be validated by the majority.

- **Consortium:** This is a form of private Blockchain where the network is not available for the general public and is entirely operated by a few individuals or an organization. Although such organizations may not accept it, these networks are pretty much centralized among the tier 1 management. In order to be a part of such networks, read the ledger or publish any block, the member must have the required level of access.

- **DApp:** In its truest essence, it is a decentralized application and the reason why it's called so is that, unlike mainstream web applications, a DApp communicates with a decentralized network rather than a centralized database server, thus making it more trustable for the end-user. These days, Ethereum is one of the go-to choices for developers to publish their DApps.

- **Ethereum Virtual Machine**: Before understanding what an EVM is, it is important for you to realize that a successful Blockchain network must always be in a state of agreement, which is achieved by reaching a

consensus. As soon as the network agrees on a new block, the state of the network changes, which is handled by the EVM that utilizes e-WASM byte-code for managing transitions. Moreover, it should also be noted that the state of the network is always the same on every node and in case if it is not, then the network is not in consensus and hence, a failed Blockchain.

- **Exchange:** It happens to be a platform where users can trade their digital assets without involving an intermediary. Some of the popular exchanges include Binance, CoinBase, Bitmex, and Bybit.

- **Gas Price:** It is important to understand this concept from the real-world example. Whenever you visit a bank and transfer the funds to another person's account, the bank acts as an intermediary and charges a certain transaction fee to facilitate the transfer. Since there is no middleman that you have to trust on a Blockchain network and every task is performed by a self-executing smart contract, the network needs a fractional amount of funds from each transaction to sustain its operations. Therefore, whenever a smart contract is executed, a transaction fee is applied which is also referred to as gas price.

- **Gossip Protocol:** As the name suggests, it happens to be a process by which the members of a Blockchain network "communicate" or rather exchange information with their peers. While the term might be funky for some people, its importance cannot be ignored as, in order to maintain the same copies of the ledger on all nodes, it is important for each node to pass on the received information to its peer. This process should be repeated for as long as all nodes have the same information. Please note that this process is recursive – implying that every time a node receives new information, the same cycle is repeated.

- **Testnet:** As the name suggests, a Blockchain protocol running on the testnet is not available to the general public and is primarily for developers' testing. The reason is that if they deploy it for the public, then instead of developing a quality platform, the developers would have to spend a substantial amount of time on addressing the bandwidth in real-time as well.

- **Mainnet:** As soon as the Blockchain is fully developed, it is deployed on the mainnet and the entire functionality is available for the mainstream users (or the public).

- **Merkle Root:** Conceptually, it is the junction where all branches of the Merkle tree meet. From a technical standpoint, Merkle root represents the hash of all transactions on the Blockchain network.

- **Public Key:** Public key is your identity on the Blockchain network as it allows you to receive funds and decrypt the messages sent to you.

- **Private Key:** Just to be clear, unlike a public key, your private key private key is now known to the mainstream public network. Although their generation and security are difficult and technical tasks, you don't have to worry about that as your wallet would do it, but these are important as a private key determines whether you have the ownership of an asset or not.

- **Secure Hash Algorithm:** It is a type of hashing function that was primarily designed by the NSA, although there are several iterations to it now (e.g. SHA256 that is used in Bitcoin).

- **Non-Fungible Token:** Essentially, it is a type of Cryptocurrency but a major distinction is that while main stream coins and tokens can be bought in fractional amounts as well, an NFT represents a unique entity, and therefore, it is never divisible. For instance, if an artist published a music file on the Blockchain network, an NFT would be assigned to that file.

D. **Types of Blockchain**

- **Public Blockchain:** A public Blockchain is a non-restrictive, permission-less distributed ledger system. Anyone who has access to the internet can sign in on a Blockchain platform to become an authorized node and be a part of the Blockchain network. A node or user which is a part of the public Blockchain is authorized to access current and past records, verify transactions or do proof-of-work for an incoming block, and do mining. The most basic use of public Blockchains is for mining and exchanging cryptocurrencies. Thus, the most common public Blockchains are Bitcoin and Litecoin Blockchains. Public Blockchains are mostly secure if the

users strictly follow security rules and methods. However, it is only risky when the participants don't follow the security protocols sincerely. Examples are Bitcoin, Ethereum, Litecoin.

- **Private Blockchain:** A private Blockchain is a restrictive or permission Blockchain operative only in a closed network. Private Blockchains are usually used within an organization or enterprises where only selected members are participants of a Blockchain network. The level of security, authorizations, permissions, accessibility is in the hands of the controlling organization. Thus, private Blockchains are similar in use as a public Blockchain but have a small and restrictive network. Private Blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc. Examples of private Blockchains are Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

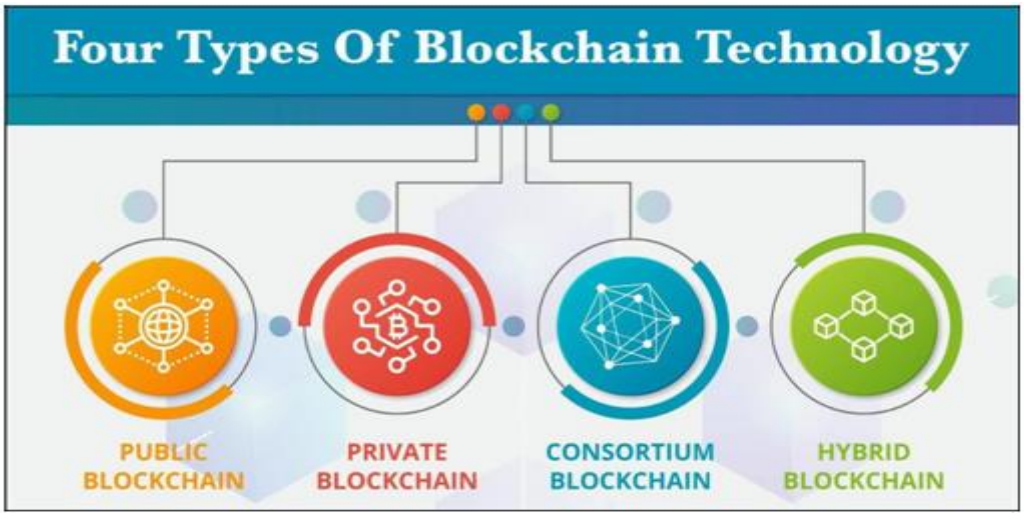

Figure 2: Types of blockchain.

- **Hybrid Blockchain:** A hybrid Blockchain is a combination of the private and public Blockchain. It uses the features of both types of Blockchains that is one can have a private permission-based system as well as a public permission-less system. With such a hybrid network, users can control who gets access to which data stored in the Blockchain. Only a selected section of data or records from the Blockchain can be allowed to go public keeping the rest as confidential in the private network. The hybrid system of Blockchain is flexible so that users can easily join a private Blockchain with multiple public Blockchains. A transaction in a private network of a hybrid Blockchain is usually verified within that network. But users can also release it in the public Blockchain to get verified. The public Blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the Blockchain network. Example of a hybrid Blockchain is Dragon chain.

- **Consortium Blockchain:** A consortium Blockchain is a semi-decentralized type where more than one organization manages a Blockchain network. This is contrary to what we saw in a private Blockchain, which is managed by only a single organization. More than one organization can act as a node in this type of Blockchain and exchange information or do mining. Consortium Blockchains are typically used by banks, government organizations, etc. Examples of consortium Blockchain are: Energy Web Foundation, R3, etc.

E. Applications of Blockchain

- **Healthcare:** Blockchain can play a key role in the healthcare sector by increasing the privacy, security and interoperability of the healthcare data. It holds the potential to address many interoperability challenges in the sector and enable secure sharing of healthcare data among the various entities and people involved in the process. It eliminates the interference of a third-party and also avoids the overhead costs. With Blockchains, the healthcare records can be stored in distributed data bases by encrypting it and implementing digital signatures to ensure privacy.

- **Government:** Blockchain technology holds the power to transform Government's operations and services. It can play a key role in improving the data transactional challenges in the Government sector, which works in siloes currently. [8] The proper linking and sharing of data with Blockchain enable better management of data

between multiple departments. It improves the transparency and provides a better way to monitor and audit the transactions.

- **CPG and Retail:** There is a huge opportunity for Blockchain technology to be applied in the retail sector. This includes everything from ensuring the authenticity of high value goods, preventing, fraudulent transactions, locating stolen items, enabling virtual warranties, managing loyalty points and streamlining supply chain operations.

II. LITERATURE SURVEY

Blockchain is an open and distributed ledger that is used to record transactions between two parties. This way of recording a transaction is both permanent and verifiable, making it one of the best ways to keep transactions. Blockchains are built on the open-source platform. Different versions of these Blockchains are possible, which are developed as per the needs of various industries. As Blockchain is a distributed ledger, every transaction is stored. on more than one computer, which ensures that every transaction will be permanent without any fear of loss. As Blockchain is distributed, it can neither be owned nor be fully controlled by a single entity. Transactions are between two parties, and no other parties are involved; this results in lower costs, and once a transaction is performed, it cannot be changed under any circumstances. This section presents the survey of current literature in the area of Blockchain. The literature in the current chapter has been gathered using academic search engines such as Google Scholar, IEEExplore, and others. The articles were searched using indexing terms such as Blockchain, Blockchain applications, Blockchain survey, Blockchain consensus, Ethereum, Ethereum survey, Uniswap, Cryptocurrency, etc. The articles were searched from the year 2008 to the year 2022. We have tried to be comprehensive in terms of publication year and sources of reports.

The section is organized as follows: Section-A presents the research of Blockchain as a technology. Section-B discusses various applications growth in enterprise operations that rely on Blockchain for improving security, transparency, and protection. Section-C presents different papers on cryptocurrency as a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority. Section-D presents Cryptocurrency trading, which involves buying and selling digital assets to make a profit. Section-E presents the development of various Decentralized Applications outside the purview and control of a single authority. Section-F presents considerable research on the Uniswap platform that uses a set of smart contracts to execute trades on its exchange.

A. 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 can be seen as the origin of the Blockchain technologies we see today. It is in this paper the Bitcoin and Blockchain revolution started. Even though the article was published as a non-peer-reviewed white paper, it is one of the most cited works in the Blockchain research area. The article itself is short and does not include so many details. It primarily presents the overall idea and structure of Bitcoin as a cryptocurrency. The report does not divulge information on the solution, the specific technologies, and the exact properties and implementation of the Bitcoin system. Another interesting note is that Satoshi Nakamoto never mentions the term Blockchain specifically in his paper. But he does talk about chains of blocks, proof-of-work chains, and lengths of chains [4].

- **Ethereum White Paper A Next Generation Smart Contract & Decentralized Application Platform By Vitalik Buterin, 2014:** The intent of Ethereum is to merge together and improve upon the concepts of scripting, altcoins, and on-chain meta-protocols and allow developers to create arbitrary consensus-based applications that have the scalability, standardization, feature-completeness, ease of development, and interoperability offered by these different paradigms all at the same time. Ethereum does this by building what is essentially the ultimate abstract foundational layer: A Blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats, and state transition functions. A bare-bones version of Name coin can be written in two lines of code, and other protocols like currencies and reputation systems can be built in under twenty. Smart contracts, cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can also be built on top of our platform, with vastly more power than that offered by Bitcoin scripting because of the added capabilities of Turing completeness, value-awareness, Blockchain-awareness, and state [5].

- **Where Is Current Research on Blockchain Technology? A Systematic Review, 2016:** Blockchain is a centralized transaction and data management technology developed first for Bitcoin Cryptocurrency. The reason for the interest in blockchain is its central attributes that provide security, anonymity and integrity without any third-party organization. Their objective was to understand the current research topics, challenges, and future directions regarding Blockchain technology from a technical perspective. The majority of research focuses on revealing and improving the limitations of Blockchain from privacy and security perspectives [6].

- **Understanding Blockchain Technology Simanta Shekhar Sarmah, 2018:** Blockchain is one of the most significant technological inventions in recent years. Blockchain is a transparent money exchange system that has transformed how a business is conducted. Companies and tech giants have started investing significantly in the Blockchain market, which is expected to be a net worth of more than 3 trillion dollars in the next five years. It has become popular because of its irrefutable security and ability to provide a complete solution to digital identity issues. It is a digital ledger in a peer-to-peer network. This paper provides a background on Blockchain technology, its history, architecture, how it works, its advantages and disadvantages, and its application in different industries [7].

- **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:** Blockchain is the underlying technology of several digital cryptocurrencies. Blockchain is a Blockchain that stores information with digital signatures in a decentralized and distributed network. The features of Blockchain, including decentralization, immutability, transparency, and audibility, make transactions more secure and tamper-proof. Besides cryptocurrency, Blockchain technology can be used in financial and social services, risk management, healthcare facilities, etc. A number of research studies focus on the opportunity that Blockchain provides in various application domains. This paper presented a comparative analysis of the trade-offs of Blockchain. Also, it explained the taxonomy and architecture of Blockchain, comparing different consensus mechanisms and discussion challenges, including scalability, privacy, interoperability, energy consumption, and regulatory issues [8].

B. **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 gained substantial attention in recent years with increased interest in several diverse fields, including the healthcare industry. Blockchain offers a secure, distributed database that can operate without a central authority or administrator. Blockchain uses a distributed, peer-to-peer network to make a continuous, growing list of ordered records called blocks to form a digital ledger. Each transaction, represented in a cryptographically signed block, is automatically validated by the network. Blockchain has also garnered interest as a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing. In this article, the authors have described the basics of Blockchain and illustrated this technology's current and future applications within the healthcare industry [9].

- **Banking on Blockchain: Costs Savings Thanks to Blockchain Technology, 2017:** Blockchain technology can optimize the global financial infrastructure, achieving sustainable development and using more efficient systems than at present. In fact, many banks are currently focusing on Blockchain technology to promote economic growth and accelerate the development of green technologies. This paper looked at the challenges and opportunities of implementing Blockchain technology across banking, providing food for thought about the potentialities of this disruptive technology. To understand the potential of Blockchain technology to support the financial system, authors studied the actual performance of the Bitcoin system, also highlighting its major limitations, such as the significant energy consumption due to the high computing power required and the high hardware cost [10].

- **Opportunities and Risks of Blockchain Technologies in Payments– a research agenda, 2017:** Authors proposed a research agenda divided into three focal areas 1) organizational issues, 2) issues related to the competitive environment, and 3) technology design issues. We discuss several salient themes within each of these areas and derive a set of research questions for each article, highlighting the need to address risks and opportunities for users and different types of stakeholder organizations [11].

- **Blockchain Technology: Implications for Operations and supply chain management, 2019:** The purpose of the authors of this paper is to encourage the study of Blockchain technology from an Operations and Supply Chain Management (OSCM) perspective, identify potential application areas, and provide an agenda for

future research. An explanation and analysis of Blockchain technology were provided to identify implications for the field of OSCM [12].

- **A Comparative Study: Blockchain Technology Utilization Benefits, Challenges, and Functionalities, 2021:** Blockchain technology enables users to verify, preserve, and synchronize the contents of a data sheet (a transaction ledger) replicated by multiple users. It has provided considerable advantages and incentives to industries to enable better services. This review explores the benefits, challenges, and functionalities that affect Blockchain applications in different sectors. This article was constructed as a systematic literature review study from 1976 articles and 168 final articles were selected and classified into three main dimensions, benefits, challenges, and functionalities, in four different sectors: government, financial, manufacturing, and healthcare. The results were extracted and compared based on factors in three dimensions, which were categorized as benefits (informational, technological, economic, organizational, and strategic), challenges (technical, organizational, adoption, operational, and environmental and sustainability), and functionalities (point-to-point transmission, data ownership, data protection, and transaction processing) [13].

- **Integrating Blockchain Technology With Internet Of Things To Efficiency, 2021:** The authors focused on integrating Blockchain technology with the Internet of Things. The study is necessary to develop practical and feasible means to improve the accuracy, accountability, and trust among various parties involved in Blockchain transactions. The study indicated a need to enhance the architecture of Blockchain and the IoT system. It shows a need to develop a new model to improve efficiency and accuracy. This research paper recommends using the decentralized model to enhance the efficiency of integrating Blockchain technology and IoT [14].

C. **Cryptocurrency as a digital currency**

- **An Analysis of the Cryptocurrency Industry Ryan Farell University of Pennsylvania, 2015:** Blockchain records individual transactions and ownership of all crypto-currencies that are in circulation, and this system is managed by the so-called Blockchain "miners. The usage of Blockchains as immutable ledgers can be seen as the origin of the Blockchain technologies we see today. This paper provides a concise yet comprehensive analysis of the Cryptocurrency industry with a particular study of Bitcoin, the first decentralized Cryptocurrency [15].

- **Cryptocurrency, Monia Milinkovic, Faculty of Economics, 2018:** The digital revolution is a change from analog and electronic to digital technology and is currently at its peak. Since we live in the digital era, it is logical that the digital form of money, cryptocurrency, has to appear. Cryptocurrency, as a digital form of cash, functions with the help of a technique called cryptography. Cryptography is a process that translates legible information into codes that cannot be broken at all. The cryptocurrency is based on the digitized so-called. The main book of all crypto watch transactions is called Blockchain. Blockchain records individual transactions and ownership of all cryptocurrencies in circulation, and this system is managed by the so-called Blockchain "miners," who have to update all transactions that have occurred and ensure the accuracy of the information. In this way, the security of the transaction is confirmed. This paper will address the theme of cryptocurrency and its role in economic growth. Types of Cryptocurrencies will also be shown, as well as their expansion in countries in transition.

- **Multiscale Characteristics of the emerging global cryptocurrency market, 2021:** The authors introduced the history of cryptocurrencies, describing Blockchain technology. Differences between cryptocurrencies and the exchanges on which they are traded have been shown consistently. The central part of this review surveys the analysis of cryptocurrency price changes on various platforms.

D. **Crypto Trading**

- **Preliminary findings on cryptocurrency trading among regular gamblers: A new risk for problem gambling, Devin J. Mills, Lia Nower, 2019:** The present results suggest that trading cryptocurrencies may appeal to gamblers exhibiting greater problem gambling severity. Future research should begin to include cryptocurrency trading in screening, assessment, and treatment protocols, particularly with regular gamblers [16].

- **Cryptocurrency Trading Using Machine Learning, Thomas E. Koker and Dimitrios Koutmos, 2020:** The authors presented a model for active trading based on reinforcement machine learning and applied this to five major cryptocurrencies in circulation. Concerning a buy-and-hold approach, they demonstrated how this model yields enhanced risk-adjusted returns and serve to reduce downside risk [17].

- **The psychology of cryptocurrency trading: Risk and protective factors Paul Delfabbro1, Daniel L. King and Jennifer Williams, 2021:** The paper examines potential defensive and educational strategies that might be used to prevent harm to inexperienced investors when this new activity expands to attract a more significant percentage of retail or community investors and suggests the need for more specific research into the psychological effects of regular trading, individual differences and the nature of decision-making that protects people from harm while allowing them to benefit from developments in Blockchain technology and cryptocurrency [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 comprehensive survey of cryptocurrency trading research by covering 146 research papers on various aspects of cryptocurrency trading (e.g., cryptocurrency trading systems, bubbles, extreme conditions, prediction of volatility and return, crypto-assets portfolio construction and crypto-assets, technical trading, and others). This paper also analyses datasets, research trends, and distribution among research objects (contents/properties) and technologies, concluding with promising cryptocurrency trading opportunities [19].

E. **Decentralized Applications**

- **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:** The authors of this paper traced the development of Blockchain systems to reveal the importance of decentralized applications (dApps) and the future value of Blockchain [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:** The authors of this paper presented the first comprehensive empirical study of Blockchain-based DApps to date, based on an extensive dataset of 995 Ethereum DApps and 29,846,075 transaction logs over them, and then proposed some implications for DApp users to select proper 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:** In this paper, the authors provided a comprehensive overview of DLT, analyzing the challenges, providing solutions or alternatives, and their usage for developing decentralized applications. They defined a three-tier based architecture for DLT applications to systematically classify the technology solutions described in over 100 papers and startup initiatives [22].

III. PROPOSED MODEL

A. **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. 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. 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.

B. **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. 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. 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.

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.

C. **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. 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. 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. 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

D. **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. 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. 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 elements.

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.

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.

IV. USER INTERFACE AND RESULT

- **Our User Interface:**

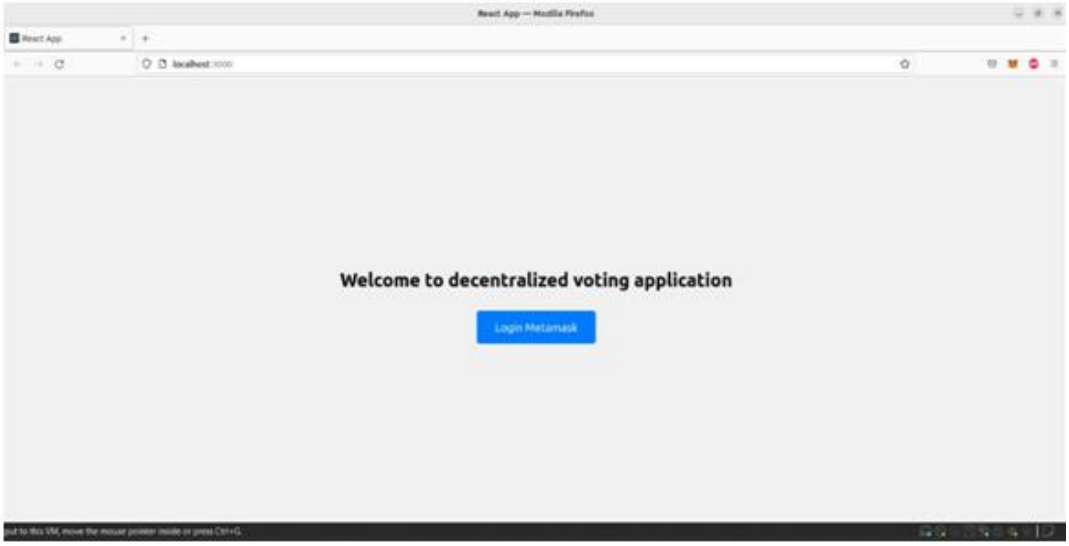

Figure 3: User Interface.

- **Connecting Wallet:**

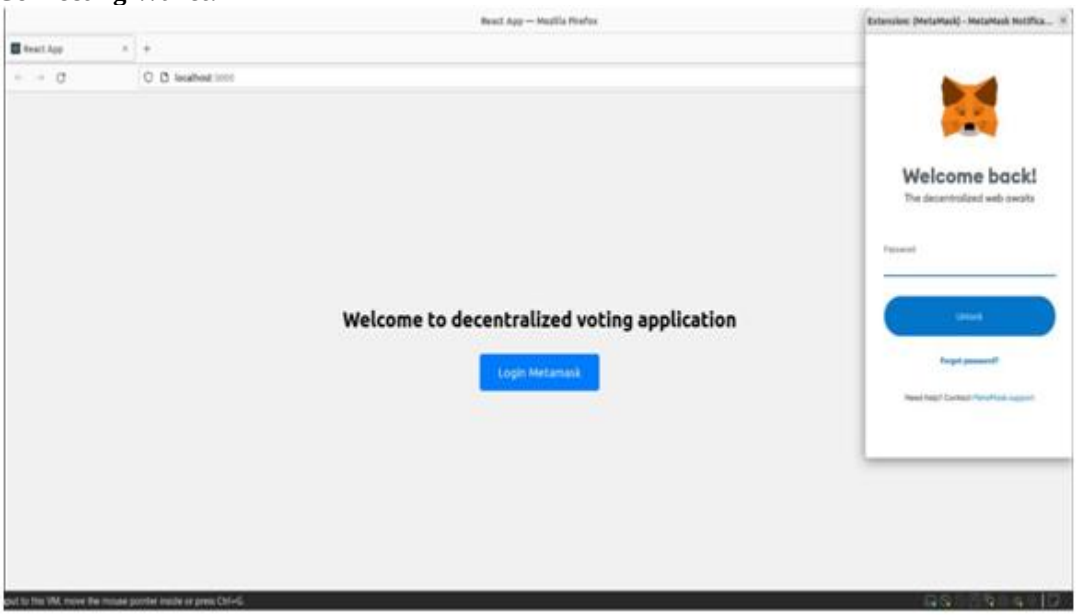

Figure 4: Connecting Wallet.

- **Connected**

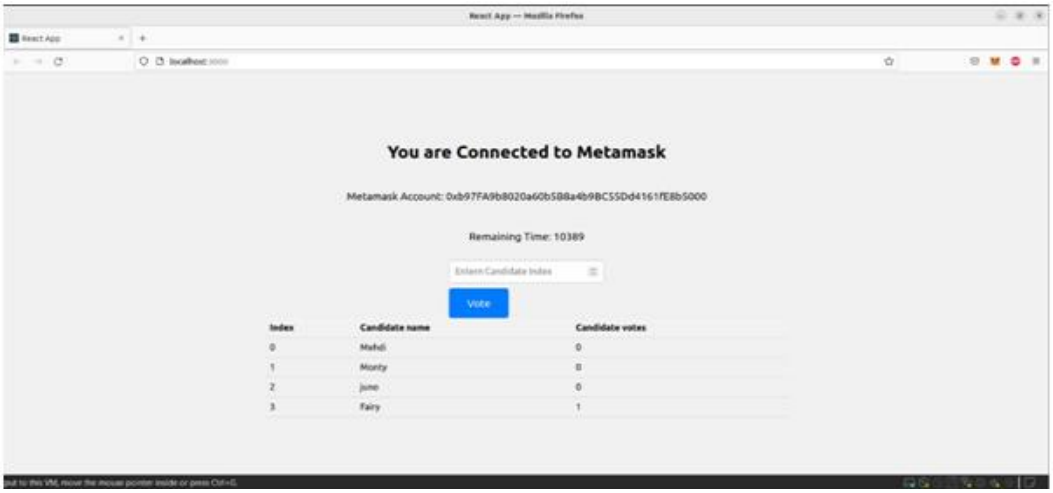

Figure 5: Connected.

- **Voting**

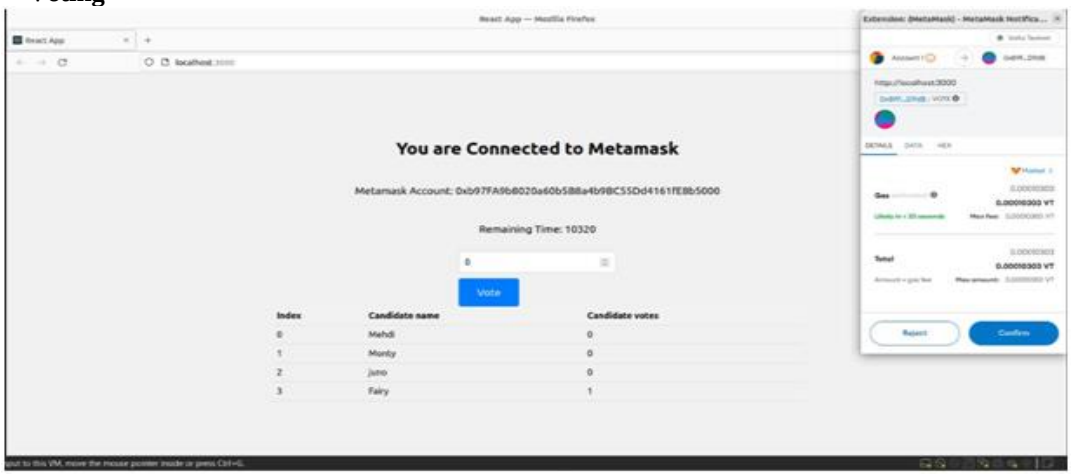

Figure 6: Voting.

- **Voted**

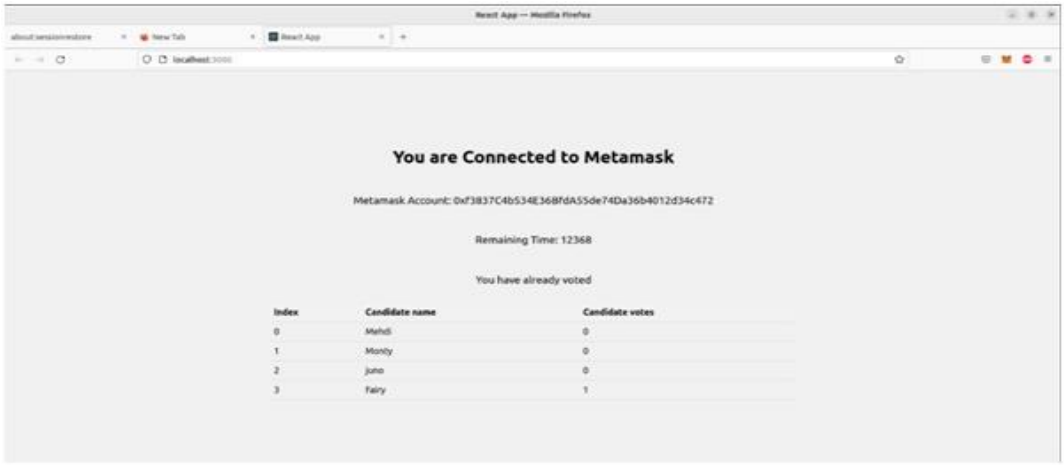

Figure 7: Voted.

- **Waiting for time to complete**

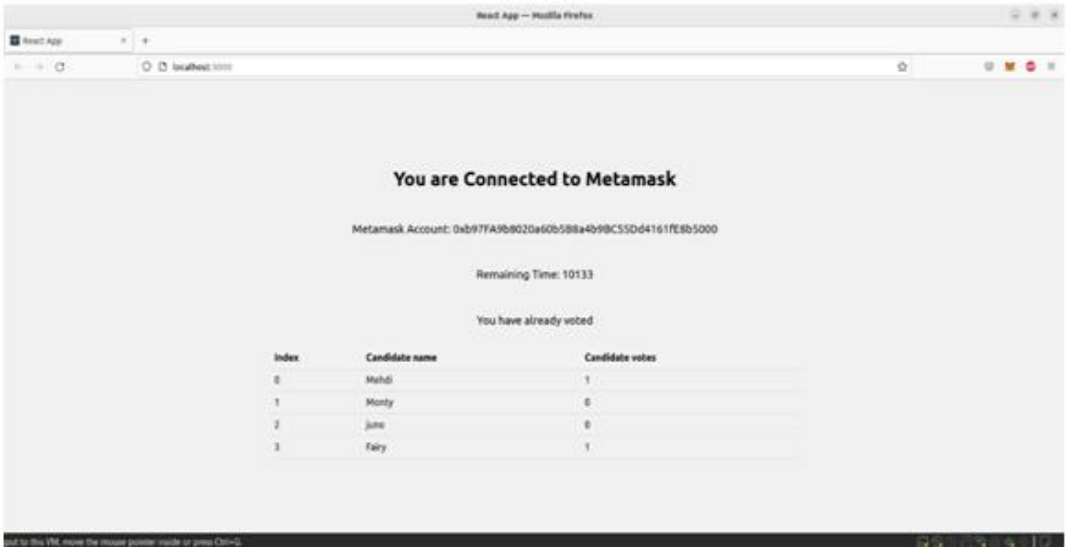

Figure 8: Waiting for time to complete.

- **Voting Finished**

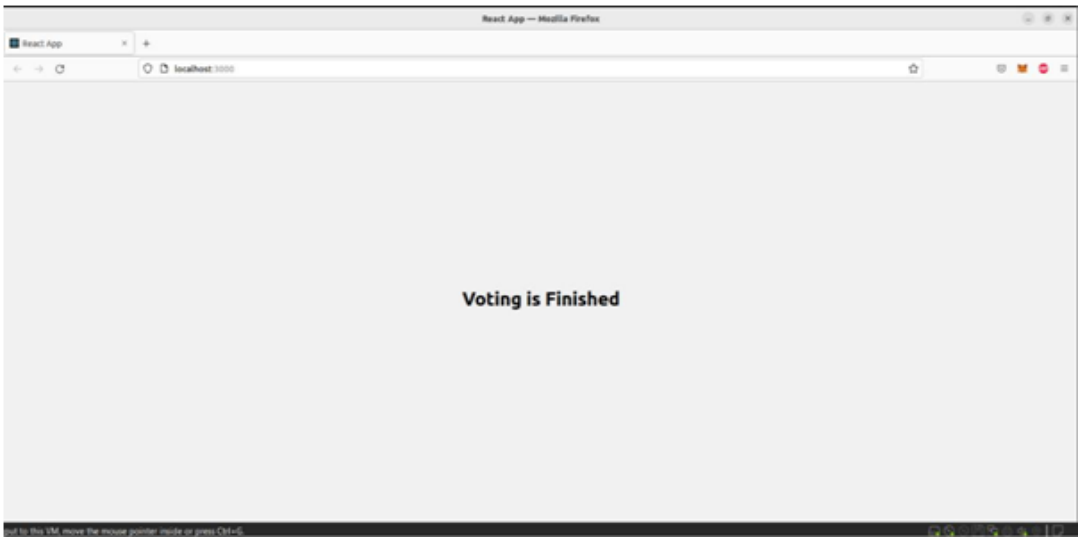

Figure 9: Voting Finished

V. CONCLUSION AND FUTURE SCOPE

A. **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.

B. **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.

- **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.

- **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