IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN BASED VOTING SYSTEM USING METAMASK AND GANACHE

[1]Hariram Srikanth
Department of Information Technology
St. Joseph's College of Engineering
Chennai, India

[2]Harikrishnan D
Department of Information Technology
St. Joseph's College of Engineering
Chennai, India

[3]Duraimurugan S
Associate Professor
Department of Information Technology
St. Joseph's College of Engineering
Chennai, India

Abstract :

Blockchain technology is an emerging and rapidly growing within recent times. Blockchain technology is popularly used in various industries across the globe. The reason behind the usage of this technology is because it is very versatile, secure and globally accessible. The trend of blockchain was introduced with the introduction of cryptocurrencies. The concept of blockchain saw a major surge with the introduction of NFTs along with the usage cryptocurrencies. Empowering the authorization and security provided by Blockchain, we have implemented a voting system using Cryptocurrencies and Ganache.

Introduction :

Blockchain has pioneered itself into the mainstream of the technology [6] with the shooting up Bitcoins which is digital cryptocurrency in and around the year of 2008. Blockchain has emerged itself as one of the leading technologies which has attracted many scientists [7] to turn their heads. A blockchain can be basically described as a decentralized immutable append-only public ledger which stores all the data and transactions between their peers in a safe and secure manner. Blockchain follows the concept of blackboard strategy where the transaction being made in a network is visible to all the individual entities present in the network. So, no transactions can be hidden or modified. Every transaction is unique and cannot be tampered with. Therefore, blockchain brings the conception of tamper-proofing to the table. Without the intervention of third parties' successful transaction can be made securely with blockchain technologies.

So as mentioned above, due to the flexibility and adaptability of blockchain, this has spread its wings across all the technologically digitalized industries like Money transfer, Financial Exchanges [9], Lending, Insurance, Real Estate [15], Secure Personal

Information, Voting, Government Benefits, Artist Royalties, Healthcare [8,12,13,16,17,19], Non-Fungible Tokens, Supply Chain Management, Data Storage. In 2021, the total capital inflows in the blockchain space were USD 30.5 Billion. In 2022, this amount was surpassed by July. The total inflows by July 2022 were USD 31.3 Billion in Blockchain investments [18]. The conclusion from this study is that many companies and governments have started to invest in the concept of blockchain [11,20] for various of the above-mentioned functions and others also. With the introduction of Web 3.0 in the mere future, blockchain is considered to rule the technology atleast for another 30-40 years.

Developed countries have implemented Blockchain in their day-to-day activities for most of the part. Developing countries needs to understand the potential and importance of Blockchain and what it brings to the table. A basic activity that is followed by every democratic country is the process of voting. Voting needs to be done in a safe and secure manner because it has the power to decide the country's fate until the next election. Safety and Security are exactly the advantage of blockchain. The main purpose of this paper is to bring

out and maximize the potential of Blockchain and its Technologies and how to implement this technology in the voting system.

Resources :

1. **MetaMask :**

MetaMask is a cryptocurrency wallet and also a decentralized application (dApp). MetaMask was created by Aaron Davis in the year 2016 by a blockchain technology company known as ConsenSys. In the span of 2-4 years from creation, MetaMask served as a E-Wallet which consisted only Ethereum coins. But due to its increase in usage and popularity, many other cryptocurrencies were also introduced in the MetaMask making it the first E-Wallet browser extension. Around the mid-2017, the Ethereum ecosystem witnessed a massive surge in its usage which resulted in the expansion to MetaMask where new and more features were added. Also in the year 2018, MetaMask App was introduced in popular mobile platforms like Android and iOS. Constant upgradation in the MetaMask software made it more user friendly and also flexible which supported many dApps. It is believed that MetaMask will play a major role in the upcoming Web 3.0 update worldwide.

MetaMask acts as a gateway between the user webpage and the Ethereum Mainnet chain allowing users to access Ethereum supported system from their local machine. The interface of MetaMask is very simple and easily understandable where the user is able to store, manage and also trade Ethereum and Ethereum based assets like Goerli, Sepolia, Linear Goerli, Linea Mainnet and many more. The main features of MetaMask include – Wallet Functionality, dApp Browser Extension, Support of Cross-Platform, Token and Transaction Management, Privacy, Safety and Security Concerns. The architecture of MetaMask comprises of the client interface which connects the Ethereum nodes to do transaction signing and managing handled by the scripts running in the background. All the data handled by the MetaMask exists on the Ethereum Blockchain Network.

It also provides safety measures like password and phishing protection, Open-source and extension permission. MetaMask application in the real-world scenarios include Non-Fungible Tokens (NFTs), Web3 Integration, Decentralized Finance (DeFi).

2. **Ganache :**

Ganache, a blockchain development environment has borrowed its name from the realm of desserts. Ganache is as important in the blockchain development as it is in the world of pastries. It is defined as a blockchain generating environment which helps the blockchain developers to build and test blockchain based applications and decentralized applications (dApps) locally from the client machine. It is a replication of blockchain environment which makes the blockchain developer create and test blockchain and its network without tampering with the actual real world blockchain environment.

Ganache provides the user with a local simulation of blockchain network which can be used remotely and consistently to test a dApp without interacting with the main network. Developers can use Ganache which provides an isolated environment to create and control smart contracts. It also has a clear and smooth interface which explains the user the structure and architecture of the locally created blockchain network without any fees. Main attraction of the usage behind the Ganache is that it provides the user with the prefunded accounts of test Ethereum (ETHs) which is not a real cryptocurrency. Test Ethereum are nothing but a pseudo cryptocurrency used for any development of a blockchain based dApp. On top of this, Ganache provides flexibility of its locally generated blockchain network by providing customization of gas price, consensus algorithm and network speed. It also has integrated and built in features that supports troubleshooting and state reversing during testing of any transaction.

Ganache is an open-source development toolkit which is often used along with any Ethereum development framework like truffle. Every blockchain integrated project or a dApp project that wants to use or access Ganache must have a Truffle-config.js file that connects the developing project to the Ganache which will create a blockchain network for this project locally. This integration of the project and the blockchain network provides a comprehensive environment for creating and debugging Ethereum based projects.

Methodologies :

1. **User :**

A legal voter should have any government proof like a voter ID or an Aadhar card. The user should have mobile number which they had used to register their government ID card. Every voter should possess an account in the MetaMask wallet. One voter should not have more than one account logged in at the time of voting. During the day of election, the government will send the voters some cryptocurrency to spend for voting. This currency can only be used for the purpose of voting and is invalid anywhere else.

2. **Authentication :**

The voter has to make sure that his MetaMask login credentials are kept confidentially. During voting in the online platform, the voter must re-enter their MetaMask login credentials in the website to verify their integrity. Once the integrity check is done, the system redirects them to the voting platform and gets them to vote using their MetaMask account. The government will have the private key address of every voter and they will be manually added in the process of voting. Note that each account will have an unique private key address and once voted, the user with the same account cannot revote again. Here the authentication of the user is checked twice.

3. **Casting The Vote :**

In the voting page, the voter will see the proposal and the registered candidate details. Every candidate in the election will have a separate page which briefs about them and their party. The user can have a clear idea of all the candidates and can make a will decisive vote. Once the voting is done, a pop-up message will brew saying that "Your vote has successfully been casted. Thank you for voting."

4. **Devices :**

Any smart device that has the ability to connect to the internet can be used here. Devices like mobile phones, laptops, tablets and computer systems are some of the key devices where the vote can be casted safely and securely. Device with anti-virus preinstalled is even more encouraged.

5. **Backend :**

Every vote casted will be stored in the blockchain network along with gas price, currency spent, mining time, transaction ID, block hash, previous block hash and time stamp to verify the legitimacy of the casted vote.

Requirement Analysis :

Functional Requirements :

1. **Digital Ballot Paper :**

Before starting the voting process, the candidates must be verified of any criminal histories before the preparation of the Ballot Paper which is used for casting the vote. During the time of voting, in the voter's interface, the digital Ballot Sheet will consist of the candidates with their respective parties along with their agenda where the voters can make a knowledgeable decision to cast their vote.

2. **Lodging Of Vote :**

With the help of the digital ballot sheet, the voter can cast their vote only for a single candidate. The casted vote is secured in a way that any vote cannot be decrypted to find the information of that vote such as the voter and the candidate favoured of that vote. To achieve this privacy and security, the system relies on encryption techniques. As mentioned above, each voter will have a unique private key where after casting, the key will get logged on and this prevents double voting. After successfully voting, the vote is recorded in the system and the count of vote against each candidate is calculated in real-time.

3. **Tallying Of Votes :**

The system will calculate the number of votes casted for each candidate in real-time and the results will be public to all the voter's interface once the admin closes the voting session. The final result page will consist of total number of registered voters, total votes and total votes for each candidate. This gives the perfect conclusion as to why a candidate won the election along with the difference in votes.

Non-Functional Requirements :

1. **Confidentiality :**

Only the voter will know the data inside the vote block and not even the admin will get the information of which voter has voted to which candidate. The admin will only get the information of the count of votes. Ergo, this intends high confidentiality to the voters and their vote which is meant to be secure.

2. **Authentication :**

In this system, only the voters registered by the admin can caste their vote and no other person who is not registered can take part in the voting process. Therefore, all the registered voters are genuine voters and this also prevents double voting as each voter will be registered only once. All the casted votes are bundled as a single block along with its data where the risk of attack is minimal.

3. **Authorization :**

The registered voter has to login to their MetaMask wallet to cast their vote. Each wallet has a unique private key and the system only opens when that wallet has been registered by the admin. Also, the voter's wallet must consist of a set of unique digital coins that will be available during the time of voting. If these coins are not present in the wallet, the voter cannot caste their vote which acts like a double authorization factor before voting. This feature proves the originality of the voter and their vote.

4. **Privacy :**

Unlike any other traditional voting system, this system does not generate any receipts or any sort of confirmation to the voter and their corresponding vote. This encourages the privacy of the vote where the spill of information is not at risk and the privacy of the vote remains only with the voter themselves.

5. **Data Integrity :**

Once the vote is casted, even the voter cannot change the data inside the vote block. The voting process is irrevocable for both the voters and even the admin. Once the vote is casted, the data is stored permanently and no further tampering can be done. This ensures high data integrity and data coherence.

Existing System :

1. **Paper Based Voting System :**

According to Electoral Office of Jamaica [2], the voting process starts 6-8 months prior of voting where the officials from the Electoral Office will visit each and every home and verify the details of each and every eligible voter and provide them with the Voter ID. After providing and completing the necessary paperwork, the Election Commission must hire representatives and train them to supervise the voting process. There should be ample of manpower required in all the voting booths available to ensure smooth and hassle-free voting process. Police officers must be allocated in all the voting booths and must maintain the discipline and decorum inside the voting campus. Before 30 mins of the commencement of the voting, the Election Commission officials must take care of all the paperwork and must have enough printed material where the voter can cast their vote. After the voting process, there is another separate group of people hired by the Election Commission where they count all the paper where the vote was casted. There is a high possibility of human error and missing the count in votes. Every count matter in the election so miscalculation during the process of counting can completely change the result of election. Also the money spent on human resources and other resources like transportation, paper, etc are high and are very time consuming processes.

The Election Commission of Jamaica have stated that they have slowly moved into digitalizing the voting process where only the information of the voters is stored on a virtual database.

2. **Iraqi Voting System :**

In the Iraqi Voting System [1], the authors have mentioned the concept of printing the ballot sheet and asking the users to mark their favoured candidate and passing the sheet through a scanning device which logs the vote and sends to the central voting server. The process first starts by validating the candidate with the voter ID and making sure the originality of the voter. Then a sheet called as the Ballot sheet which consists of all the registered candidates. The voters are asked to shade the circle next to the favoured candidate's symbol. After the voter marks this with an ink, the ballot sheet is produced into a scanner device where the whole ballot sheet is scanned. When the scanner finds the shaded circle, the corresponding candidate's count of vote is incremented by one in the central voting system and the vote is casted successfully.

3. **Smart Card In Voting :**

In smart card based voting system [3], all the voters are provided with a smart card or a voter ID where a machine readable chip will be present. In the temporary voting booths also known as kiosks, a voting machine will be present where the voter inserts the cards into the machine. After reading the chip in the card, the voting machine retrieves all the user information and provides them with an interface of casting the vote. All the registered candidates will be present on the monitor of the machine where the user has to press the button to cast their vote. After casting the vote, a beep message is heard which means successful voting and the voter can remove their card. This is just like an ATM where the ATM is connected to the bank server via a network, similarly, the kiosk is also connected to the central voting server where the vote is added. There are no privacy or authentication in this type of voting system. Anyone with the smart card can cast the vote. Also the network where the kiosks and the central network are connected can be crashed by trafficking the network with high volume of transactions and the voting process can be disrupted.

4. Blockchain Based Voting :

In the Blockchain based voting system [4], proposed by the authors, the voter has to login into the system with their thumb impression. The thumb impression must be registered with the voter ID to do this process. If the match is found, the voter will be redirected to another page where the list of all the registered candidates will present and can continue with the voting process. If the match is not found, the voter is a malicious user and the voting system immediately shuts down. After the fingerprint is scanned, the voter's data is gathered and the system fetches the candidates who are registered in the constituency where the voter's address indicates. Only those candidates will be present along with their party's symbol. Each vote is considered as a unique transaction. After casting the vote, the miners will start to mine a new block where the new transaction will be added. Every transaction will have a unique ID and a unique block hash.

Coming to the security aspects, this system uses a cryptographic hash block to ensure end-to-end encryption. Each block will have unique block hash and if the hash is already logged, then the system will automatically reject the transaction. When the fingerprint is recorded, the transaction also contains these details so if the voter tries to vote again, the voter's fingerprint will be detected and denies further access. After completely completing the voting process, the user will receive a tracking code where the voter can track their vote. This code cannot be used to find any details regarding the information of the vote. Even the admin cannot find out the details of the vote with this tracking code. The tracking is rather seen as confirmation of the vote and provides the voter with a satisfaction that their vote was casted. This also improves the verifiability of the system where the voter feels trusted and that their vote is counted.

Proposed System :

The voting process needs to be digitalized to encourage all the voters and also to increase the percentage of the total voting counts. Even though there are many systems that are proposed, they all have the major drawbacks of scalability and security threats. The main drawback of the online voting systems is that they all can be easily prone to security attacks and are more vulnerable. The only reliable way of proposing an online voting system is with the help of blockchain based voting. This model easily overcomes all the security threats and the drawbacks of most of the proposed system. Blockchain based transaction is identified to be the most trustable way of transaction due to its encryption algorithms and asymmetric key cryptography techniques. All the existing cryptocurrencies that are worth trillions of US Dollars are all based blockchain based transactions. Even though blockchain based transactions are time consuming, they are the perfect way to overcome all the security threats and vulnerabilities that exist. Blockchain based transactions are hashed in such a way that they cannot be traced back to the original data of the transaction even if the block is made public. No one, except the user themselves can have access to the block who possess the secret private key of each block.

Even though there exists an idea of blockchain based voting system in real world, they also have drawbacks. The main drawback of the system are the miners where they will have to keep mining a new block where the transactions must be stored. During a normal general body election, there will be millions of people voting at the same and the network overhead is very high. The miners must be quick enough to solve the puzzle and mine a new block within seconds which is near to impossible. To mine a new block, the miners should possess a high-end high-performance system which can only solve a puzzle within minutes to hours. And so, if the rate of mining new blocks is slow, the voting process is delayed up to few days or even weeks. This is a major flaw in the existing blockchain based voting system.

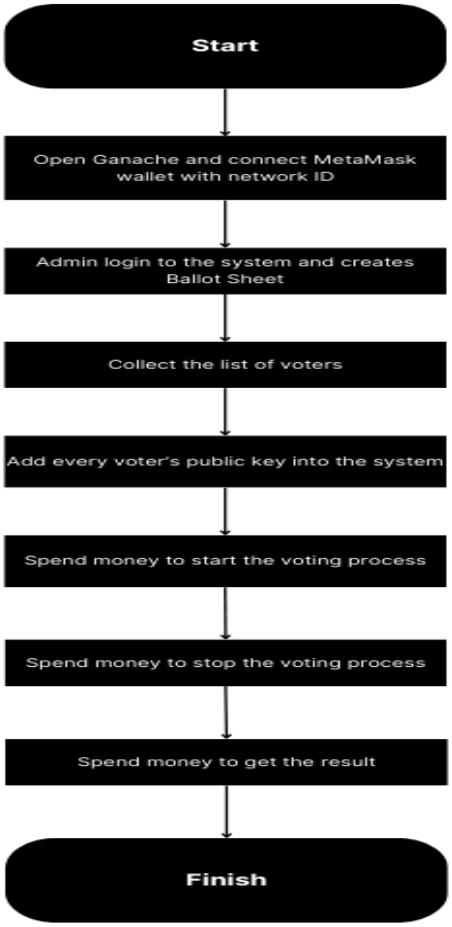
Our system overcomes all these proposed challenges by simply using a MetaMask wallet instead of complex mining of new blocks. The MetaMask is an e-wallet where the world-renowned cryptocurrencies can be stored. In our system, the MetaMask wallet is used to store the cryptocurrencies that can only be used at the time of voting and is invalid elsewhere. Each and every cryptocurrency will have a public and a private key where the user has to login into the wallet in order to spend the coins to vote. Each vote is considered as a transaction in blockchain based voting and hence, the need to spend to coins acts as a double verification to each transaction. This proposed system is remotely accessible to anyone who has an access to a laptop or a desktop. The main purpose of the online based voting is improving the total rate of voting and our system is the best way to implement online based voting system with high security and encouraging everyone to vote.

Working :

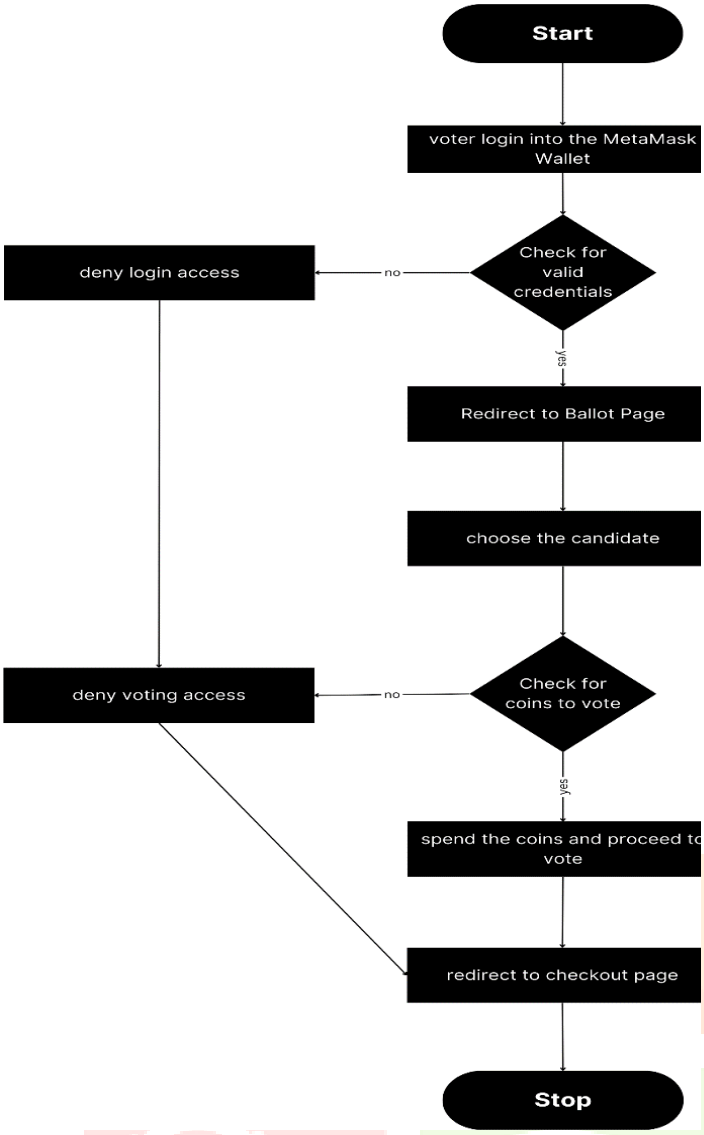
Although there are many other online voting systems are proposed and are existing, the main problem with the proposed models are the security issues. The authentication, authorization and integrity of the model are at risk. No model properly addresses these drawbacks and the security threats that arise along with them. The proposed system of this model overcomes all the other proposed system drawbacks and also has its own advantages on top of that. The proposed system starts with the admin where the admin has to create a

MetaMask wallet account and login. After entering the system, it is the duty of the admin to create the ballot sheet with all the registered candidates. After successfully adding the ballot sheet, the admin starts to register all the verified voters. Only the voters registered by the admin are eligible to take part in the voting process. Even though this process is time consuming, the security and the integrity of the voting system is achieved at the highest level. After adding all the eligible voters, the admin starts the voting process. Till this process is completed, the voters will not be able to enter the voting system. After the admin starts the voting process, the voters will now be able to enter into the system where they will have login with their MetaMask account. There will be a username password which exist for each MetaMask account where they will to enter in order to access their wallet. This process proves the authorization of the system where if the private key of the voter's MetaMask account is not added by the admin, then they will not be able to take part in the system. All these registered MetaMask account will have some spendable cryptocurrencies, where they should spend the coins in order to cast their vote. These cryptocurrencies are invalid anywhere else except this system therefore it cannot be spent anywhere. These currencies possess no value to actual real-world currencies and simply exist to help with the transaction of the voting process.

After casting their vote, the voters can either log out of the system or can wait until the voting process is done and the results are published. The admin after a certain time, decides to end the voting process and as soon as the voting process is over, all the voters can immediately view the results of the election with total number of votes for each candidate and the difference between the votes. This proves the authenticity of the system which provides the voters with the complete transparency of the number of votes casted against each candidate. The working of the system ends by showing the results of the election and providing all the voters with the complete transparency of the process. Even though the voters will be able to view the total count of votes against each candidate, they will not get the information as to which voter casted their vote to which candidate. The vote and the data of the vote is supposed to be private with the voter themselves. So, this system achieves that through encryption protocols and that even the admin cannot get the data of the vote. All the votes are considered as transactions and all these transactions are committed into a blockchain with unique block hash. So, this encourages the authentication drawbacks of the other systems and overcomes them. Finally on top, the interface of the system is very simple and easy to understand. Any average citizen with an average knowledge about modern gadgets can easily understand the working of the system. This system also negates the problem of double voting. When the user logs in into their MetaMask account and spends the coins to votes, the system will immediately log this transaction in the chain and even if the user tries to login again, the system will be closed showing the message that the particular voter has already casted their vote.



Workflow of admin process



Workflow of voter process

System Analysis :

Advantages :

- Remotely Accessible : This system encourages every citizen to vote. The main problem in reduce in the total number of votes is availability. People have migrated to different parts. This system motivates all these people to vote from their house.
- Easy user interface : Another main problem when it comes to online voting is a complex voting process. Our system proposes a very easy and a simple user interface.
- Improved safety and security : Unlike the traditional system, this system brings authorization, authentication and integrity with encryption techniques.
- Ensures privacy with transparency : Even though the data of votes are hidden, this system provides the total count of votes to all the voters.
- Elimination of double-voting : This system eliminates the process of double-voting by detecting a MetaMask account if logged in again or all the coins are spent during the first original vote.
- Errorless calculation : The drawback of human-made voting calculation is neglected and only provides accurate results.
- Faster and easy process : Since there is no mining activity, the process is fast and with simple UI, the process is made very easy.
- Reduced cost and manpower : Even though the developing cost of this software will be costly, it is one time investment and if purchased, the human effort can be completely neglected.

Disadvantages :

- Human and network error : Admin can miss out one or two voters during the process of adding. The network can be vulnerable to DDos attacks.
- Availability of devices : This system can be a problem to rural areas where the availability of a computer system or a laptop is very rare.
- Lack of knowledge : There will be some people who will not know the idea of blockchain and refuse to vote. Also basic computer knowledge is required to vote.
- Admin work overload : The admin has the highest workload of anyone which includes preparing the ballot sheet and also adding the voter manually.
- Scalability issues : The transfer from small scale to large scale may require a few modification and extra network security.

Conclusion :

The main purpose of this proposed model is that there already many ideas and many working models of an online based voting system. This proposed system, takes it to the next level by introduced new and unknown concept like MetaMask, Ganache and also cryptocurrencies for voting. The inclusion of blockchain for this purpose will completely turn the fortunes and suddenly the online voting system feels achievable and implementable in real-world scenario. The system addresses all the security and privacy issues found in other systems. We still have no idea how the election results may turn out if 100% of the citizens cast their vote. Maybe in future with this proposed system, people are motivated to vote and we can finally witness complete voting by all citizen which can even change the fate of any country. Even though there are

drawbacks in this system, with a minor scrutiny and repair in scalability issues, it can reach to its apex exertion and serve its purpose for the betterment and welfare of our society.

Future Works :

This system can be further enhanced by improving its major drawbacks. The first main drawback of this system is that the admin has to enter every voter manually. This can be automated with a simple read write query along with a database. Another area for improvement can be confirmation of vote to voter's mobile or email just acknowledging that they have casted their vote successfully. Further works can be made to convert this into a mobile app which can be accessible to anyone because there are many mobile phone users. A close study in the amount of spending coins can be done to exactly provide with the voters for only one vote. Double verification can be done with fingerprint or retinal scans which can be synced with the voter ID. With more experienced and knowledgeable developers all these can be achieved and can make the system more prevalent than it is now.

References :

[1] Wasan Salman, Viktor Wakovlev and Sameer Alani (2021) "Analysis of the traditional voting system and transition to the online voting system in the republic of Iraq"

[2] Electoral office of Jamaica (2007), Available from www.jis.gov.jm/special_sections/election_2007/index.html

[3] Deville, D et al (2003), "Smart Card Operating system: Past, Present and Future". Proceedings of Fifth USENIX/NordU Conference, Vasteras, Sweden

[4] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan (2017) "Secure Digital Voting System based on Blockchain Technology"

[5] Mohammed Dabbagh, Mehdi Sookhak and Nader Sohrabi Safa (2019) "The Evolution of Blockchain: A Bibliometric Study"

[6] Satoshi Nakamoto. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System"

[7] S. Makridakis, A. Polemitis, G. Giaglis, and S. Louca, (2018) "Blockchain: The next breakthrough in the rapid progress of AI"

[8] K. Fanning and D. P. Centers, (2016) "Blockchain and its coming impact on financial services"

[9] I. Eyal, (2017) "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities"

[10] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz (2018) "On blockchain and its integration with IoT. Challenges and opportunities"

[11] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han (2018) "When intrusion detection meets blockchain technology: A review"

[12] Y. Zhang, and J. Wen (2016) "The IoT electric business model: Using blockchain technology for the Internet of Things"

[13] J. Zhang, N. Xue, and X. Huang (2016) "A secure system for pervasive social network-based healthcare"

[14] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo (2018) "Blockchain: A panacea for healthcare cloud-based data security and privacy?"

[15] A. Schaub, R. Bazin, Omar Hasan, and L. Brunie (2016) "A trustless privacypreserving reputation system"

[16] R. Dennis and G. Owenson (2016) "Rep on the roll: A peer to peer reputation system based on a rolling blockchain"

[17] M. Nakasumi (2018) "Information sharing for supply chain management based on block chain technology"

[18] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani MeDShare (2017) "Trust-less medical data sharing among cloud service providers via blockchain"

[19] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito (2018) "Blockchain and IoT integration: A systematic survey"

[20] D. Tapscott and A. Tapscott (2017) "How blockchain will change organizations"