Voting System Using Blockchain (Face Recognition)

Gaddam Harsha Vardhan[1], Swapnil Shah[2], Vanshika Gupta[3], Rohithreddy.B.C[4], Tanya Bisht[5]

Abstract - *As we have comprehend that casting a ballot extortion is basic in India and moreover in created nations as nicely. There were some sports to lessen casting a poll misrepresentation, for example utilization of EVM machines in India. What in the event that we can make use of a few innovation to ensure in opposition to something comparable. Here comes the utilization of Blockchain, a block chain is a blanketed conveyed report that is consistent and makes use of cryptographic techniques to execute the given houses. In this project we plan a proposition for putting in the first-class solution for a block chain casting a ballot dApp that consolidates citizen self-sovereign-ID and plain balloting form arrangement. We will make use of superb agreements to execute the requirements installation by way of the Election fee of India. Our proposition has a tendency to the essential standards and indicates key capacities and contemplations for a totally supported drive and progressed elector turn out to be, progressing commitment, and amazing rate investment finances by using limiting errors and guide facts passage and framework corporation for heritage frameworks. We be given that an electronic democratic dApp ought to be purpose driven, nearby area situated, in view of open recommendations for block chain advancements, citizen protection and safety as a purpose, and self-sustaining test and ease for polling form corporation.*

Keywords—Blockchain, Dapp, smart contract, Multi-factor authentication, truffle suite

1.Introduction

Across democracy, electoral protection is an trouble of country wide security. The laptop safety area has been operating at the possibilities of digital voting machine, with an aim of decreasing the fee of election and growing the safety of the election. From the start of the democratic elections,the voting machine become primarily based on pen and paper.Instead of pen and paper currently the Indian election makes use of evm machines,that are liable to vote casting fraud and device tampering.Electronic voting machine are taken into consideration invalid and anybody with bodily get entry to that device can tamper with the gadget ,as a result affecting all votes casted.

Enter blockchain era. A blockchain is a disbursed, immutable, incontrovertible, public ledger. This new technology works thru 4 foremost capabilities:

(i) The Blockchain ledger is distributed and no single birthday celebration controls it:the allotted ledger and no unmarried point of failure.

(ii) Once a transaction is delivered to the ledger it can't be edited or deleted.

(iii) Any proposed "new block" to the ledger have to reference the previous model of the ledger, creating an immutable chain from where the blockchain receives its call, and for this reason stopping tampering with the integrity of previous entries.

(iv)The majority of the nodes should reach a consensus before a transaction is brought to the block.

1.1 E-voting

The E-Voting system especially entails the implementation of two of the most mentioned input and counting services within the academic and commercial international. In order to have a at ease vote the following systems must be considered and should be nicely maintained.

Fairness: Voting outcomes must not be introduced earlier than the quit of the vote casting technique. This will make certain that the ultimate citizens will not be encouraged to vote.

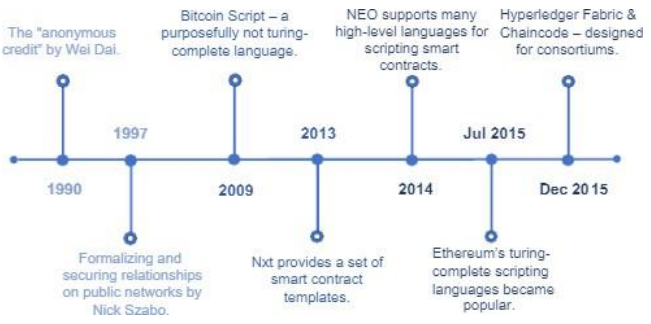
- Eligibility: Ensure that most effective eligible electorate need to be allowed to vote.

- Confidential: Once a voter has voted, the info of the entered vote need to no longer be disclosed to different customers.

- Verification: This asset enables voters to make certain that the entered vote is counted or no longer. There are kinds of verification: man or woman authentication and wellknown[7]. Individual verification exams the weather votes solid by way of people selected for the calculation system or not. And if possible established verification any person can affirm the election consequences once they may be published.

- Exemption: The power of voters to trade or convert citizens to vote after inclusion.

1.2 Three Blockchain as a Service



The blockchain innovation was provided in 2008 when Satoshi Nakamoto made the primary virtual cash referred to as Bitcoin. The Bitcoin blockchain innovation makes use of a decentralized public file joined with PoW(Proof-of-Work)based totally stochastic consensus conference, with economic motivations to report a completely asked succession of squares, the blockchain. The chain is imitated, cryptographically marked and freely verifiable at each change so nobody can mess with the records that has been composed onto the blockchain. The blockchain shape is an affix simply information shape, with the cease intention that new squares of data can be stored in contact with it, but cannot be adjusted or erased. The squares are fixed in order that each square has a hash this is an element of the past block, giving the confirmation of permanence. Though the Bitcoin blockchain distributes all additives of the complete chain, in normal one-of-a-kind varieties of blockchain may be public, non-public or consortium based totally. Public blockchains award admittance to peruse and capacity to make an trade to any client in that agency. This type is for the maximum part applied for cryptographic styles of money (e.G., Bitcoin, Ethereum, Dogecoin and Auroracoin). Consortium blockchain is a "incompletely decentralized" blockchain, where the agreement interplay is confined by way of a pre-chosen set of hubs. Envision a consortium of 15 economic businesses, every one among which works a hub of which 10 must signal every block all collectively for the rectangular to be valid. The choice to pursue the blockchain can be public or limited to the contributors. Private blockchain limits the compose access in addition to the read access also, to specific participants who can check their alternate inner. That makes the exchange on a personal network much less pricey, since they just ought to be confirmed by way of no longer many hubs which can be depended on and with ensured high handling electricity. Hubs can be depended on to be all around related and shortcomings can swiftly be constant by means of manual intercession, allowing the utilization of agreement calculations which give absolution after an awful lot more limited rectangular activities.

1.3. Four Smart Contracts in Blockchain

Smart contracts may be created and despatched to diverse blockchain systems (e.G., Ethereum). Different platforms provide a ramification of features to construct clever contracts. Bitcoin, Ethereum and Hyperledger Fabric are a number of them. Bitcoin is a blockchain platform that supports cryptocurrency transactions. Bitcoin uses a bytecode scripting language based on a completely restrained set of laptop terms.Bitcoin writing language can guide the advent of complex agreements that comprise logical understanding.Like Bitcoin, Ethereum, it is a blockchain and cryptocurrency. In addition, the ability to transfer cash helps the construction and implementation of complicated structures primarily based on clever contracts within the blockchain. The basic unit of the Ethereum system is an account. At Ethereum there are styles of bills: outsourced bills and contract accounts. The first is managed by means of the corresponding private key holder and continues stability. It can also be used for transactions to switch cash or to go into right into a smart settlement. Later good judgment code good judgment is controlled and has balance, retention and status. At the heart of Ethereum is the Ethereum digital machine, which makes clever contracts. The clever settlement source code is compiled into a bytecode form that may be translated by using a visual Ethereum device. Each Ethereum node operates the equal command to simplify smart contracts and block blockchain protocols. Smart Ethereum contracts are built in one-of-a-kind Turing languages consisting of Solidity.

Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

2. Related Works

We are utilizing blockchain generation. Blockchain is a secure and lasting appropriated technique that could document change actions among clients. Blockchain become made by way of Satoshi Nakamoto in 2008 who is regarded in the Bitcoin exchange records base framework. Bitcoin itself is a coins whose exchanges make use of the Internet to organize and rely on cryptography for records secrecy troubles and, manifestly, protection on the hour of the alternate. Blockchain itself has a decentralized framework by way of appropriating all statistics to numerous materials with the aim that members in the enterprise can participate with out the requirement for endorsement from the focal substance. Decentralization at the blockchain lets in each worker to partner and has a comparable element as shaping a type of friend to peer community. For this situation, facts following is easier, and while one worker, there may be a reinforcement impedance that is with none trouble finished by way of any other worker, and the unsafe worker is in short eliminated from the blockchain network. Methods offered on this report had been very one of a kind and progressive in evaluation to the evaluate carried out for the paper. New implementations for the UI/UX have been accomplished; separate flow charts had been designed after thinking about the New South Wales Voting gadget which become diagnosed with a completely negative type of person interface. The SHA 256 field was used inside the encryption for securing the machine in order that no adversary can access the votes with out the authorization. New Concusses blocks have been designed because of the want for improving the decentralized ledger based totally blockchain device. The technique proposed is an onchain peer voting protocol preserving some assumptions in thoughts and protocol contains one of a kind ranges that are voting ,validation on chain by using clever contract and then verification on patron through peers and final degree is revoting of ballots encrypted by the dishonest friends public key.This protocol additionally uses distributed tally method so that the remember remains same for all the friends. The

technique used on this paper is to acquire the achievement in statistics security control it's miles carried out the usage of distinctive protocols like e-verification the use of electoral Id then verification of the tokens given to the electorate.This token works to make a variety in the selection box.

The third level of the selector inserts the token into the gadget, and then the display screen will display the candidate to be selected. To vote, just genuinely press the candidate's image.

The fourth stage of each election result could be encrypted using blockchain generation to produce valid effects. In the ultimate level, after data encryption, the monitor will at once show the brief gain of each candidate.In this paper proposes to use a Homomorphic signcryption device which is suitable for mystery transmission between multiple senders(electorate) to one receiver(authority) and messages encrypted through equal encryption key and distinct signature keys are allowed to perform homomorphic computation .HSE vote casting only allows registered citizens to vote, and ensures that each voter can vote only as soon as, which can be guaranteed by way of Authentication Centre in step with Voter's ID quantity and time stamp of every poll and it is able to additionally be displayed on bulletin board which presentations the voter identification and timestamp of every poll , subsequently making sure transparency in view that bulletin board is obtainable by way of all and sundry.

2.1 Blockchain as a provider for e-vote casting

In this paper, we studied existing digital balloting systems, blockchain-based totally and evaluated their respective wishes and concerns for imposing a countrywide e-balloting gadget. Based on this, we devised a blockchain-primarily based digital voting device. In the subsequent subsection, we begin by identifying the jobs and additives for imposing an e-balloting smart settlement.

2.2 Election as a Smart Contract

Defining a smart contract includes figuring out the roles that are worried within the settlement and the special additives and transactions in the settlement system. We begin via explaining the election roles observed by using the election system

1) Election Process: In our paintings, every election is corresponded by using a smart settlement which holds the info of the birthday celebration and their consultant that are going for walks for the elections in a particular constituency. A clever settlement is deployed for each constituency ,so more than one smart settlement are deployed .There are three foremost sports in election manner:

● **Election introduction**

Election fee of India creates the election ballots using clever contracts and Dapp (decentralized software) .The app interacts with the smart contract while the vote is casted through the voter.The nearby corresponding district officer is given access to the smart agreement to rely the vote casted In this paper, we studied existing digital balloting systems, blockchain-based totally and evaluated their respective wishes and concerns for imposing a countrywide e-balloting gadget. Based on this, we devised a blockchain-primarily based digital voting device. In the subsequent subsection, we begin by identifying the jobs and additives for imposing an e-balloting smart settlement. Election as a Smart Contract

Defining a smart contract includes figuring out the roles that are worried within the settlement and the special additives and transactions in the settlement system. We begin via explaining the election roles observed by using the election system

1)Election Process: In our paintings,every election is corresponded by using a smart settlement which holds the info of the birthday celebration and their consultant that are going for walks for the elections in a particular constituency. A clever settlement is deployed for each constituency ,so more than one smart settlement are deployed .There are three foremost sports in election manner:

● Election introduction

Election fee of India creates the election ballots using clever contracts and Dapp(decentralised software) .The app interacts with the smart contract while the vote is casted through the voter.The nearby corresponding district officer is given access to the smart agreement to rely the vote casted

2.3 Voter registration

In India every eligible voter is assigned a voter ID card which is used by voter to cast the vote.In our work ,we proposed using aadhar card for the voter verification because it is extensively ordinary and has specific identification elements like fingerprint,face and cellular variety as nicely.

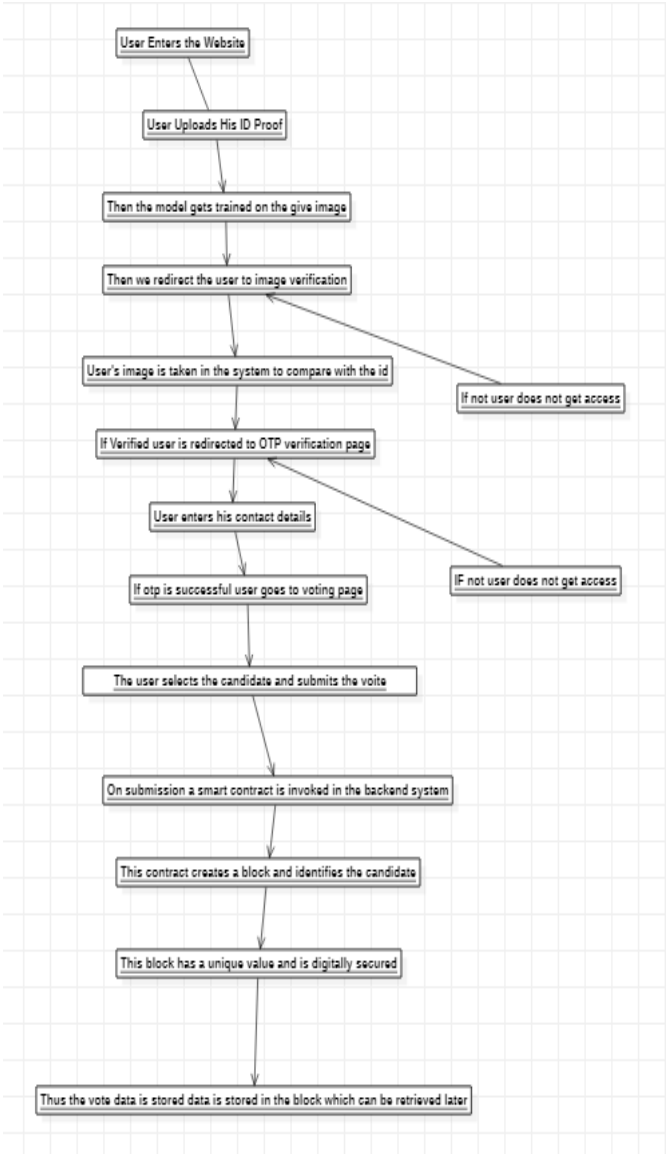
● Vote transaction

When an character votes at a balloting district, the voter interacts with a ballot clever agreement with the same vote casting district as is defined for any character voter. This smart agreement interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain.Each transaction at the blockchain holds information about who become voted for, and the vicinity of aforementioned vote.

● Tallying consequences

The Election commissioned appointed officer interacts with the blockchain and the usage of a pre-described feature calculates the very last tally of the votes.

3. System Architecture



To present a strategy for validation, our proposed framework is intended to make use of digital ID validation the usage of multi aspect authentication, which begins with facial popularity of the voter, observed by way of an OTP verification, following this system makes positive that the voter is very well vetted before the voter is let to vote. Then the person selects the candidate and submits the vote, this movement triggers into a clever agreement being invoked in the backend of the proposed device.This settlement creates a block and identifies the candidate and this block has a completely unique price and is digitally secured and thus the vote records is secured in this block that may later on be retrieved.

Here in this device architect complete work-go with the flow is expressed. The complicated integration of all technologies is shown in a detailed way. Web3js, Truffle suite, Ethereum based totally blockchain.

3.1 Module Description

To introduce a technique of at ease authentication in our paintings we are able to be using deep mastering version to seize the face of the voter in actual time and compare it with the aadhar card image of the voter. To add a further layer of safety the device will also carry out otp/e-mail verification of the voter.

1) A kiosk gadget on the balloting sales space plays the specified verification approaches.If the verification is successful the smart agreement similar to the district of the voter is triggered.

2) After the voter has casted his/her vote that vote along side the time stamp and other necessary parameters is introduced to the blockchain corresponding to that election.

3) After the election procedure is completed the votes may be counted the use of the smart agreement technique and additionally may be counted in real time by the administrator.

3.2 Authentication

We accompanied multi-aspect authentication to make certain user who is attempting to exercise his right to vote is who he claims to be and has a legitimate identity.First step of multi-thing authentication is facial authentication. Here the Voter is needed to add the required identification card and continue on , then this part of the device verifies whether or not the image at the ID is matching with the image this is seen on the digital camera.Then the user is redirected to the login page that is on a exceptional server , we use the concept of microservices here.If the identification fails to suit the person , isn't always redirected to the server which hosts the voting utility.If the voter's authentication is verified, the consumer is redirected to the server which holds the vote casting utility, there the voter has to go into an e-mail identification and then the consumer gets an OTP to the given e-mail, on the way to be tested. If the consumer is authenticated, the user is given the choice to exercise the proper to vote.

3.3 Face Recognition

Facial Recognition is a totally upcoming phenomenon because of the upward push in AI era. Recent advances in automatic face evaluation, sample popularity, and gadget learning have made it feasible to broaden computerized face recognition systems. The rapid development of facial recognition is because of a aggregate of features: the

effective improvement of algorithms, the availability of massive-scale facial records, and the manner to test the overall performance of face reputation algorithms. There are numerous unique algorithms for facial popularity, a few which we have discussed in advance.

Eigenface is one of the maximum investigated methods of facial popularity. It is also referred to as the expansion of Karhunen- Loève, eigenpicture, eigenvector, and the most important component. According to mathematical phrases, eigenfaces are the principle components of the floor distribution or eigenvectors of the covariance matrix of a set of facial photographs. Eigenvectors are instructed to symbolize exceptional values of version, respectively, among the faces. Each face can be represented with the aid of a right away price combination of the line of the eigenfaces. Blockchain It is the era of decentralized structures which permits to expand the System to huge networks of computer systems referred to as nodes related to each different and each laptop have a ledger to preserve tune of the sports within the Blockchain network. It is also a completely secure alternative for implementing a vote casting utility, every interest is stored linearly, chronological order. After a block has been covered at the quit of blockchain, it's extremely problematic to hint again and exchange the voting content of the block unless greater than half of reached a very last nation to do so. That's because each block includes its own hash, along with the hash of the block before it, as well as the formerly referred to time stamp. Hash codes are created through a math characteristic that turns digital statistics into a string of numbers and letters. If that statistics is edited in any manner, the hash code adjustments as well. This prevents any authority to adjust the device in any manner and lets in common guy to offer their votes efficiently. The evolution of voting is vital. Such technological moves forward are inevitable and welcome, at least for a country like India that has almost a billion voters. Blockchain has the ability to bring transparency in vote casting at the same time as preserving security and anonymity. Also, effects may be collected and processed speedy and straight after the balloting is finished. The not unusual voters, however, may struggle to understand this sort of technology. In truth, commonplace human beings depend a great deal on the establishments and additionally on their political leaders. We realize that the EVM debate were given momentum repeatedly within the Smart Contract

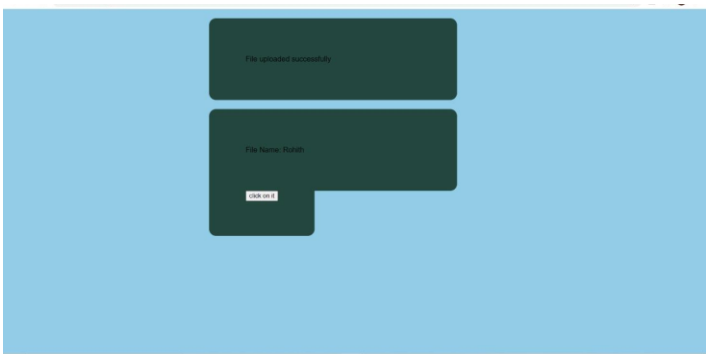
The smart contracts are examples of agreements conveyed on the Ethereum blockchain (Buterin, 2015) albeit the time period become to begin with authored earlier than (Szabo, 1997) on the subject of electronic change conventions between outsiders at the Internet. This stores the recommendations which:

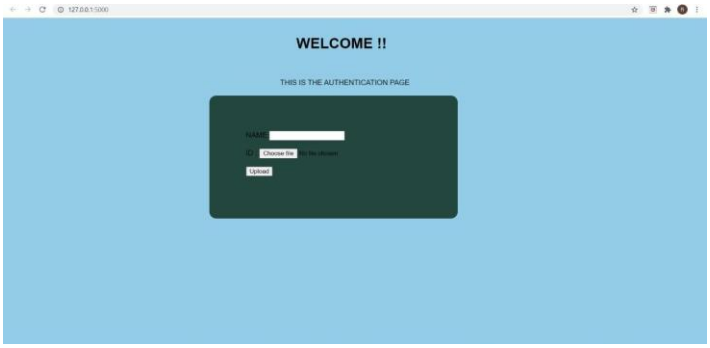
1. Arrange the provisions of the agreement,

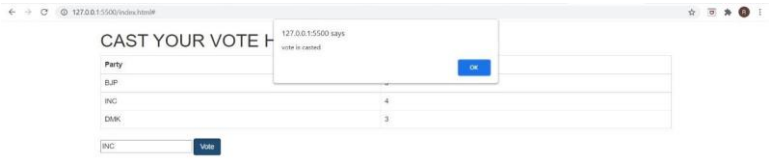
2. Consequently test the agreemen

Blockchain, mixed with clever agreement innovation gets rid of the dependence on the focal framework among the trade parties. Since the super agreements are put away on the Blockchain, each one of the associated events within the business enterprise have a duplicate of them. It can execute the concurred positioned away cycle whilst activate by way of an authorized or concurred occasion.[10] All settlement exchanges are placed away in sequential requests for future get right of entry to alongside the total evaluation trail of occasions. In the event that any collecting tries to exchange an agreement or trade at the Blockchain, any last gatherings can pick out and prevent it. On the off danger that any accumulating comes up brief, the framework keeps on operating without a deficiency of records or respectability. It, thusly, makes a solitary big secure PC framework with out the risks, fees and agree with issues of an included version.

3.4 Implementation Screenshots







3.5 Conclusion

As mentioned inside the paper the intention of our undertaking is to create a totally functional dapp that is primarily based on blockchain and smart contracts. The primary purpose become not handiest to create a relaxed machine but become to create both a relaxed, reliable and scalable machine. In order to decorate the safety of our project we've used person identity and face matching verification, and also we've got an otp verification device to test the identification of the user. The foremost feature of blockchain is to create an immutable machine so that when a vote is casted it cannot be tampered with the aid of any adversary. Now to tackle the issue of scalability and reliability which is very critical in a rustic like India with a big populace which in flip will cause huge server loads. We have targeted on developing a microservices based structure which in turn facilitates us to scale our server extra successfully and which may be utilized in real time eventualities.

We additionally plan to containerize the application the use of docker and docker-compose and use box orchestration tools like Kubernetes and OpenShift.To make sure that no longer a single vote is misplaced because of server crash or another calamity we are able to use Kafka or RabbitMQ to manage the real time information which may be added to the blockchain while the server is capable.

3.6 References

1) Ahmed Ben Ayed “A conceptual secure blockchain based Electronic voting system”International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2018

2) W. Zhang et al., "A Privacy-Preserving Voting Protocol on Blockchain," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 401-408, doi: 10.1109/CLOUD.2018.00057.

3) E. Febriyanto, Triyono, N. Rahayu, K. Pangaribuan and P. A. Sunarya,"Using Blockchain Data Security Management for E-Voting Systems”,2020 8th International Conference on Cyber and IT Service Management (CITSM),2020

4) Cristina Satizábal, Rafael Páez, Jordi Forné, Secure Internet Voting Protocol (SIVP): A secure option for electoral processes, Journal of King Saud University - Computer and Information Sciences, 2021, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2020.12.016

5) Praveen M Dhulavvagol, Vijayakumar H Bhajantri, S G Totad, Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application, Procedia Computer Science, Volume 167, 2020, Pages 2506-2515, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.03.303