Received Date: 1st November, 2022
Accepted Date: 12th April, 2023

Voting System with Artificial Intelligence and Blockchain

Sudip Bhujel[1*], Sulove Bhattarai[2], Nikesh Neupane[3] & Santosh Adhikari[4]

[1]Department of Electronics Engineering, Thapathali Campus. E-Mail: sudip.732419@thc.tu.edu.np
[2]Department of Electronics Engineering, Thapathali Campus. E-Mail: sulove.732419@thc.tu.edu.np
[3]Department of Electronics Engineering, Thapathali Campus. E-Mail: nikesh.732419@thc.tu.edu.np
[4]Department of Electronics Engineering, Thapathali Campus. E-Mail: santosh.73642@dmc.tu.edu.np

***Abstract*—Voting is an essential democratic practice of finding out the public opinion about the policy of candidates. For freeand fair voting procedure, a systematic voting system must be designed. Today almost every aspect of our lives is aided by the technology and with the advancement in the technology, the voting system can be upgraded to AI Voting System from the traditional ballot paper system with fair results. This paper discusses designing of voting system with best possible secure way. AI and Blockchain are two underlying technologies used to achieve secure and fraud-free voting environment. Face recognition being the source of truth for authentication and authorization and Blockchain encryption being the safest way to store and read electronic ballot make system ideal. All data related to voting are encrypted in Blockchain decentralized network. In blockchain technology, each process is controlled by Smart Contract, they are trackable and irreversible.**

***Keywords* — AI (Artificial Intelligence), API (Application Programming Interface), Blockchain, Face recognition, Hash, JSON Web Token, Neural Network, QR (Quick Reference) Code,Smart Contract.**

I. Introduction

Electronic voting uses electronic means to either aid or take care of casting votes. For the basic concept of electronic voting, it is convenient to divide it into four basic steps in an election process: ballot composition, in which voters make choices; ballot casting, in which voters submit their ballots; ballot recording, in which the system records the submitted ballots; and tabulation, in which votes are counted [1]. The voters usually cast votes with the aid of a touch screen display or click of a button.

Depending on the implementation, e-voting maybe use electronic voting machines (EVM) or computers which are connected to the Internet. It may encompass a range of Internet services, from the basic transmission of tabulated results to full functioning online voting through household devices i.e. mobile phone. The degree of automation may be limited to ballot composition (or choosing) or maybe a vote recording, data encryption and transmission to servers, and tabulation of the results. An e-voting system must maintain the strong requirements associated with security, accuracy, integrity, privacy, auditability, accessibility, and cost- effectiveness.

Electronic voting can be comprised of technology like punched cards, bio-metric scan voting system etc. It can also involve the transmission of ballots and votes via private computer networks or the internet.

In general, two main types of electronic voting can be identified:

- E-voting: This voting is conducted with the aid and supervision of the representative of governmental or independent electoral authorities.
- Remote E-voting via the Internet (I-voting): In this voting, voters would cast their choices from any computer connected to the Internet from any location [2].

Electronic voting technology intends to speed the counting of the ballots, reduce the cost for the manpower and can provide improved accessibility to the differently abled voters. Results can be reported and published faster. The citizen groups far from the polling station can be benefitted from the I-voting.

A. Deep Neural Network

A neural network is a network or circuit of neurons, or in a modern sense, an artificial neural network, composed of artificial neurons or nodes. Such systems “learn” to perform tasks by considering examples, generally without being programmed with task-specific rules. For example, in image recognition, they might learn to identify images that contain cats by analyzing example images that have been manually labeled as “cat” or “no cat” and using the results to identifycats in other images.

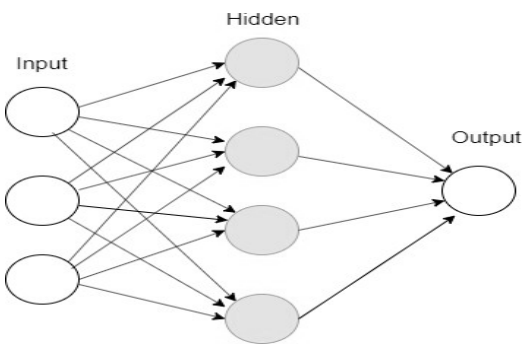

Fig. 1. Simple Neural Network with single hidden layer.

* Corresponding Author

A neural network with more than one hidden layer is Deep Neural Network, it captures more features of objects and is quite accurate. Each node in the layer has weights and gets updated in the backward propagation of neural networks on each iteration to match actual output. The deep neural network needs a lot of computational power. Most of the neural network uses a vectorized implementation of numerical calculation which saves lots of computational power.

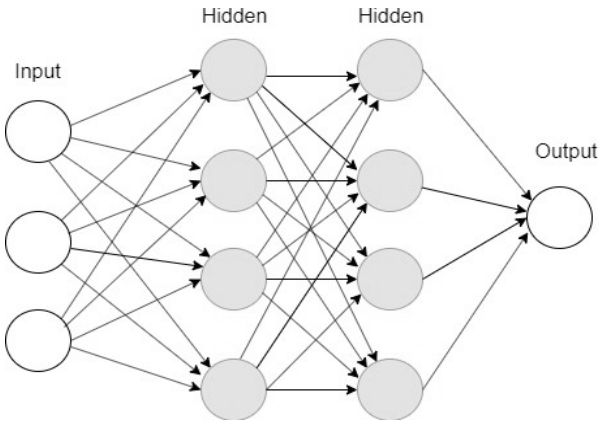

Fig. 2. Deep Neural Network with more than one hidden layer.

B. Face Recognition

There are many ways to detect and recognize faces. Some of them are feature-based, appearance-based, knowledge-based, etc. The implementation of deep learning neural network resides in the appearance-based algorithm. The deep learning gives the power to build recognition biometric software that is capable of uniquely identifying or verifying a person. All this because deep learning methods can leverage very large datasets of faces and learn rich and compact representations of faces, allowing modern models to first perform as well and later outperform the face recognition capabilities of humans.

The most popular algorithm for detecting a face is the Viola-Jones algorithm. This algorithm is popular because it was a robust real-time face detector and it can recognize the face even when rotated with 30 degrees. This algorithm is so popular because it was the first robust real-time face detector. In the mentioned method, the authors present a heuristic method in using AdaBoost classifier and Haar-like features to distinguish sub-images containing a face from non-face sub- images [3].

One of state-of-the-art face recognition algorithm is packed into Dlib c++ library. The model has an accuracy of 99.39% on the Labeled Faces in the Wild benchmark. The Dlib is a modern c++ toolkit containing machine learning algorithms and tools for creating complex software in c++ to solve real world problem. The tools and machine learning algorithm provided by Dlib library is used in face recognition python module.

The face recognition module provides an API to load image, find all face in the image, face landmarks, compare faces, etc. The comparing of face acts as face recognition. The face image of the user already registered in database is compared with the recent image from the camera, then the compare face API will provide either true or false values based on two images. This module provides parameter called tolerance value. The default tolerance value is 0.6. The tolerance value is useful in avoiding multiple matches for the same person, it might be that photos of different person may look very similar. The low tolerance value makes face comparison strict.

C. Blockchain

Blockchain is a data structure used to create a decentralized database or a ledger. Blockchain is a way of storing digital data, in which data is stored in the form of blocks, which is chained together using hashes [4]. A block is composed of a set of transactions, a hash of the previous block. So, the chain is created as every block consists of hash of the previous block. There is no central authority for the database structure which is the most powerful aspect of the blockchains. The different types of blockchains are:

- Public blockchains: Public blockchains are fully decentralized, with no individual having the authority to control the transactions that are recorded in the blockchain. Anyone is allowed toparticipate as users in this system and the transactions are fully transparent [5].
- Private blockchains: Private blockchains are alsoknown as permissioned blockchains. Participantsneed consent to join the networks. The transaction is private and is only available to the ecosystem participants.
- Hybrid blockchains: In this blockchain, the privacy benefits from private blockchain are included with the transparency and security of the public blockchain. It is a combination of centralized and decentralized features [6].

1) Blocks

Block stores information about transactions such as date, time, etc. It stores the information on who is participating in transactions. Different blocks are chained by using the hash. Block stores the hash generated by the previous block, which helps to maintain the security of the system.

2) Hash

A hash is a function that converts an input of letters and numbers into an encrypted output of a fixed length. A hash, like a nonce, is the backbone of the blockchain network. Hashes are of a constant length which is used to identify the input [7]. A hash is created using algorithms like Secure Hashing Algorithm- 256 (SHA-256).

3) Smart Contracts

A smart contract is a self-enforcing agreement embedded in computer code managed by a blockchain. The code contains a set of rules under which the parties of that smart contract agree to interact with each other. Smart contracts provide mechanisms for efficiently managing tokenized assets [8]. Generally, a smart contract is developed in Solidity. It is a self-executing contract with the terms of the agreement between the sender and the recipient being directly written into lines of code. The code and the agreements contained therein exist across a distributed blockchain network. The code controls the execution, and transactions are trackable and irreversible. A contract is declared using the contract keyword along with an identifier, as shown in the following:

```
Contract SampleContract {
}
```

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, the legal system, or an external enforcement mechanism.

4) Ethereum Network

Ethereum network is a decentralized network mainly used to transfer money and store data. There are many different Ethereum networks such as the Main Ethereum network, Kovan network, Rinkeby network, etc. The network is formed by one or more nodes. Each node is a machine running an Ethereum client. Anyone can run a node. Each node can contain a full copy of the blockchain. The 'blockchain' is a database that stores a record of every transaction that has ever taken place.

5) Transaction

The transaction in the Ethereum network consists of a nonce, address of recipient account, amount of 'Wei' (small unit of Ether), amount of Wei that the user is willing to pay for computation of his/her transaction, units of gas that the current transaction can consume, vrs data used to cryptographically encrypt the transaction and the data that is generated from sender's private key.

TABLE 1

TRANSACTION IN THE ETHEREUM NETWORK

nonce	How many times the sender has sent a transaction
to	Address of account this money is going to
value	Amount of 'Wei' to send to the target address
gasPrice	Amount of Wei the sender is willing to pay per unit gas to get this transaction processed
gasLimit	Units of gas that this transaction can consume
v	Cryptographic pieces of data that can be used to generate the senders account address. Generated from the sender's private key.
r	
s	

6) Nonce

The transaction in the network is validated by the node. The validation process is quite complex and the process is expensive. The validation process of a series of transactions inthe block is called mining. The benchmark time for mining theblock should around 15 seconds that means block time. The block time is maintained by varying the nonce. The has value of the block is continuously checked whether it is less than theparticular limit and the block time is measured. If it is around 15 seconds, the limit set fixed. So, the nonce is variable to make a hash less than the limit, and sometime it may beleading zero.

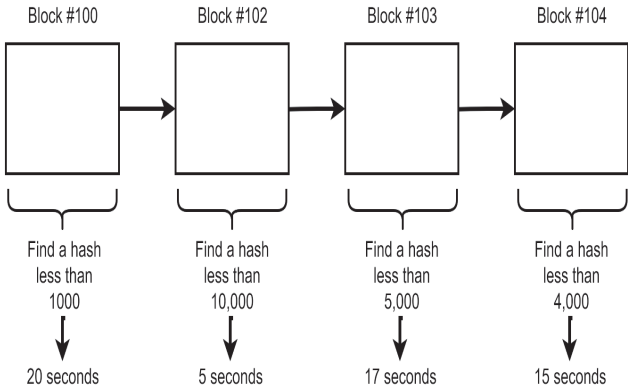

Fig. 3. Block Time, an arbitrary block time calculation.

The nonce is varied to achieve the hash of the block to be less than the limit value or target value. The limit value should be reasonable so that the block time is around 15 seconds.

7) Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs that govern the behavior of accounts within the Ethereum state. Solidity was influenced by C++, Python, and JavaScript and is designed to target the Ethereum Virtual Machine (EVM).

II. ARCHITECTURE

The overall project can be divided into two parts viz. user authentication with AI and decentralized environment with blockchain. In the user authentication process, a voter is validated using his/her unique ID and image verification. In the second part, the voters will be given a digital ID card containing demographic details and private key of an Ethereum account. The voter can request a ballot paper with their ID card, and the voter can vote for the candidate. The submitting of ballot paper makes blockchain transaction to update the voter's and candidate's details stored in decentralized network.

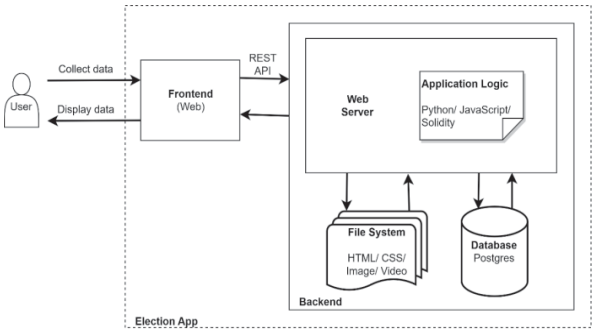

Fig. 4. Project Architecture Diagram

The User, Frontend, Backend are the main entities of the system.

- **User**: The end-user of the election app is Voter. The user requests the backend server through the frontend. The user requests data and server responses to the frontend web interface.
- **Frontend**: The responsibility of the frontend is to collect the data from the user and pass it to thebackend as a request through the REST API. Thebackend might process, store, and return the data. The frontend makes use of responses from the backend. The frontend is a web interface where the user interacts.
- **Backend**: The backend services heavily serve data and web content like HTML, CSS, images, etc. The webserver in the backend serves thestatic content like HTML, CSS, images, videos, etc. The web server is comprised of application logic. The application logic requests the database for data retrieval, creation, deletion, and updateas per the user's need. The business logic is defined on application logic to perform on the user's data.

The project implements two step verification for better security. It begins with a request from the user to login to the system and system checks for validity of user. Then, second phase of authentication starts with real-time video of user,then the system applies AI algorithm and authenticates if user is valid.

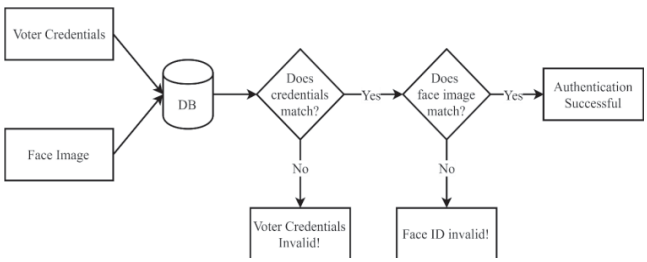

Fig. 5. User authentication process (two factor authentication)

The back and forth of user interaction and machine learning algorithm verify the valid voter to cast their vote. The authentication process begins with a user's unique ID and other relevant information, if that information is valid, the camera takes an image as an input. The algorithm then aligns the face to feed it into the algorithm. If an image is matched, the user is authenticated.

The voter fills election form. The admin or the staff validates the voter based on the data/information included in the election form. The election form includes all the demographic details with a copy of the citizenship card. Once the voter is validated then the admin creates the Ethereum accounts for that voter. The QR code is generated using the citizenship number and private key provided in the account creation. The QR code is sent to the voter.

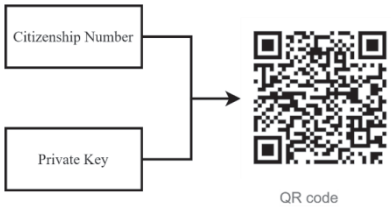

Fig. 6. QR Code of Citizenship Number and Private key

The voter can cast their vote using a QR code after verifying their face once the voting process is initiated.

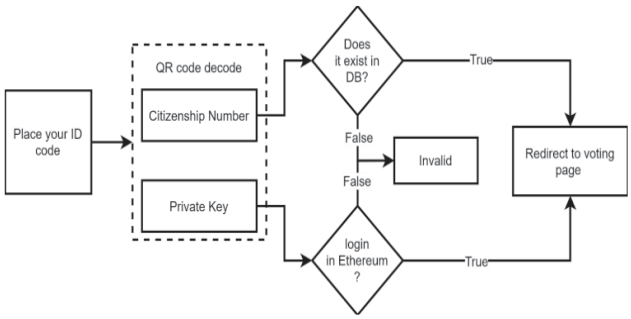

Fig. 7. Implementation Details of the Voting System

After two factor authentication of the voter, the voter will be prompted to the Ethereum network interface. The voter should place their QR code. The QR code is decoded and the citizenship number is checked whether it exists in the database or not. The system will try to login to the Ethereum network with the private key. If the Ethereum login is successful returns a positive instance, then the user is redirected to the voting page where the voter can cast vote for their candidate.

The list of verified voters and candidates are stored in the Ethereum contract in the registering phase. When the voting phase is initiated, the manager cannot add the voter and candidate anymore. The access to the ballot of the contract is restricted to those voters who are verified. The Election contract in the Ethereum network provides many restrictions based on the role. The contract will reject all the requests coming in from unlisted voters and candidates.

A. Election Smart Contract

The election contract has its variables and function defined

in it to provide a ballot for verified voters and candidates only.The address of the manager will be the address who creates an election contract. The solidity programming language hasits data structure and the election contract uses full advantages of it. The state variable is used to provide restrictions after the contract is deployed such as the manager can't add voter or candidate once the contract goes to the voting phase. The othervariables with a brief description are mentioned below.

TABLE 2
VARIABLES IN ELECTION SMART CONTRACT

Variables	Data type	Description
manager	address	Address of the person who is managing the smart contract.
voters	mappings	Address of the voters.
candidates	mapping	Address of the candidates.
state	enum	State of voting process {created, voting, ended}
totalVoter	uint	The total number of voters.
voteDropped	uint	The total number of votes dropped.
totalCandidate	uint	Total number ofcandidates.

The functions defined in the election contract provides many facilities to the manager and voters. The manager can add the voters, candidates, initiate voting, and end voting. The voter only can cast their vote if the state of the election is inthe voting phase. The verified voter can cast their vote only if the manager starts the voting phase. Once the manager starts the voting phase then he also can't add the voter and candidate. The functions defined in the election contract are listed with the description below.

TABLE 3

FUNCTIONS IN ELECTION SMART CONTRACT

Functions	Descriptions
Constructor	Constructor function with the name of the election.
addVoter	called when the manager wants to add the verified voter.
addCandidate	called when the manager wants to add the verified candidate.
removeVoter	called when the manager wants to remove the voter.
startVote	called when the voting procedure is going to be started.
doVote	called when the voting procedure is started.
endVote	called when the voting procedure is ended.

Once the manager starts the voting phase, the start Votection is called which sets the state variable to voting. The doVote function facilitates the voters and the candidates can cast their vote. The manager can only end the voting phase by calling endVote function.

The struct keyword is used for voters and candidates. The fields defined for voters and candidates are listed below.

TABLE 4

VOTER STRUCT

voterAddress	address	Address of registered voter.
isVoter	bool	True if the voter is verified.
voted	bool	True if the voter voted the candidate.

When the manager adds the voter address, the system automatically sets isVoter property true and voted property false.

TABLE 5

CANDIDATE STRUCT

candidateAddress	address	Address of registered candidate.
isCandidate	bool	True if a candidate.
totalVoteCount	uint	The total vote dropped to the candidate.

When the manager adds the candidate with candidateAddress, the is Candidate property set to true, and totalVoteCount property set to 0. The candidate is also a voter so, the address of the candidate is listed on the voter list.

III. RESULT AND ANALYSIS

The system provides voter registration and verification interface. On the registration phase, the voter is asked to provide their real-time video to enable two factor authentication. After successful verification process, the voter is provided an ID card. It will have information of voter and most importantly, it will have QR code in which the private key of the Ethereum account and citizenship number is encoded.

Fig. 8. Voter's ID Card, required for casting vote

The voter needs to go through different verification steps to cast vote. It starts with providing correct citizenship number and password. And then, they need to verify their face with real-time video input. After that voter will have rights to request for ballot paper with provide ID card. Finally, they cancast their vote.

A. Ethereum transaction

The Ethereum transaction receipt has different information such as transaction hash, transaction index, block number in the blockchain network, block has, gas used to compute the nonce, contract address, logs and status of the transaction. The status '1' signifies the success and '0' signifies failure. Thetransaction receipt is shown below,

{

"transactionHash": Hex Bytes ("0x80e934228a0fc860210bfb43 ee416b4ccfcd1 e4f5bf1e7e7 00c4177e0b16d2c9"),

"transaction- index": 0,

"blockNumber":3,"blockHash": HexBytes(

0xb27cbbbc3a27d8e25fd47620bafdd0a962880

b8664e3566 22493c9c9cd679dd9"

),

"cumulativeGasUsed": 21678,

"gasUsed": 21678, "contractAddress": HexBytes (

"0xd863E96F90A172E0F1a82f2a2952ec5a

60DADddD"

),

"logs": [],

"status": 1

}

B. Error Analysis

The sources of error might be insufficient balance in the Ethereum account for processing vote, old and outdated face image in the database, false data entry by the voter, etc. The ID card has Ethereum account private key. This account must have sufficient balance to cast vote. The insufficient balance gives an error to the voter.

The system provides two-factor authentications with face recognition mechanism that needs updated face image so that the system recognizes face in the login process. The user with outdated face image stored in database might get problem in login. The voter needs to update their face in the database time to time to get rid of authentication problem.

The authentic information should be provided in the election form. The false information and details may lead to unverified account, and may lead to no access to cast vote. The voter can update their information and details and can request for re-verification.

REFERENCES

[1] R. Peralta, "Electronic voting," ENCYCLOPEDIA BRITANNICA, 23 May 2016. [Online]. Available: https://www.britannica.com/topic/electronic-voting. [Accessed 2019 December 2019].

[2] D. L. Dimitrios Zissis, "Securing e-Government and e- Voting with an open cloud computing architecture," *Goverment Information Quarterly,* vol. 28, no. 2, pp. 239-251, 2011.

[3] M.Y.M.R.K. Pooya Tavallali, "An Efficient Training Procedure for Viola-Jones Face Detector," *International Conference on Computational Science and ComputationalIntelligence,* pp. 828-831, 2017.

[4] S. Kansal, "ibm," 03 April 2018. [Online]. Available: https:// www.ibm.com/. [Accessed 26 December 2019].

[5] "dragonchain," dragonchain, 18 April 2019. [Online]. Available: https://dragonchain.com/blog/ differences-between -public -private-blockchains/. [Accessed 26 December 2019].

[6] M. Walker, "Distributed Ledger Technology: Hybrid Approach," *Front-to-Back Designing and Changing Trade Processing Infrastructure,* 2018.

[7] J. Frankenfield, "Investopedia," 15 August 2019. [Online]. Available: https://www. investopedia.com/terms/h/hash.asp. [Accessed 26 December 2019].

[8] S. Voshmgir, "Backchaining Berlin," July 2019. [Online]. Available: https://blockchainhub.net/smart- contracts/. [Accessed 26 December 2019].