VoteBlok

BLOCKCHAIN GOVERNMENT ELECTION SYSTEM

Murad Mikayilzade, Mert Yapucuoglu, Ahmet Turan Bulut

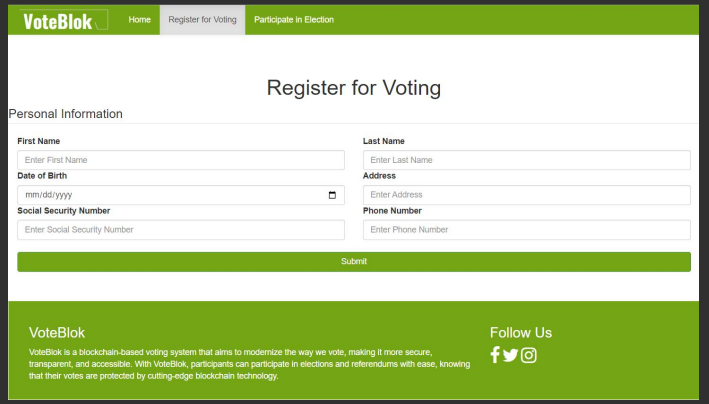
What is it?

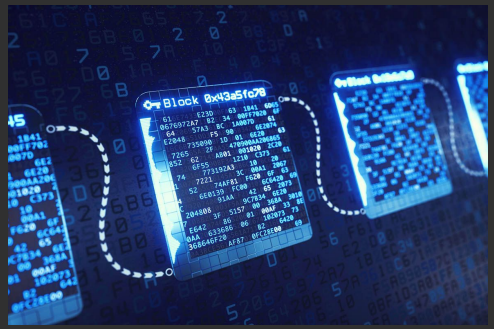
Outside:

- Website
- Safe, tamper-proof, transparent voting

Inside:

- Ethereum based blockchain
- Government database
- API





Why bother?

- Alternative, easy-access voting
- Environment friendly
- Anonymous
- Tamper-proof
- Confirmable

Doesn’t it Already Exist?

There are other “blockchain voting” systems available.

BUT

They are not fully developed solutions for elections

How is VoteBlok Different?

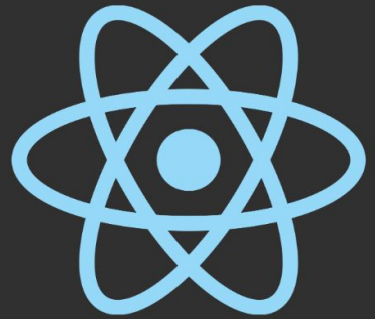
A full election process containing:

- 3 webpages
- A database
- An API
- A blockchain contract
- Some security measurements

Our Stack

What we use to deliver our functionality:

- React front-end
- Firebase database and API
- Ethereum Smart Contract
- Solidity

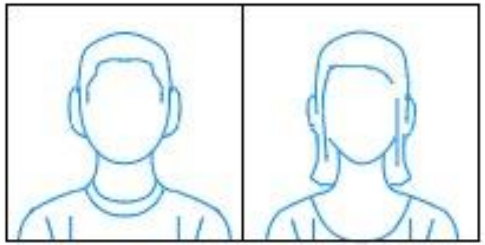


Firebase

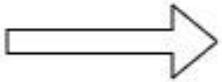
How Does It Work?

1. Candidate Creation
2. Voter Registration
3. Voting
4. Results and Confirmation

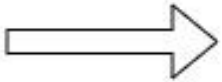
CANDIDATE CREATION



VOTER REGISTRATION



VOTING



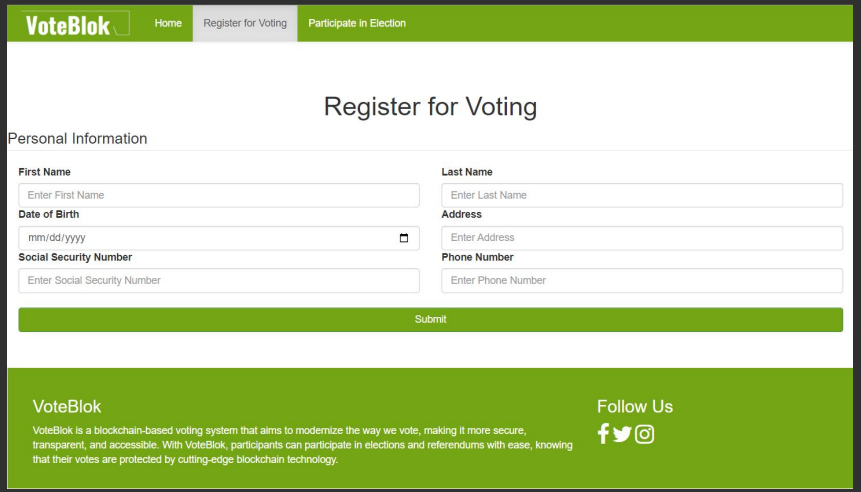
ELECTION RESULTS

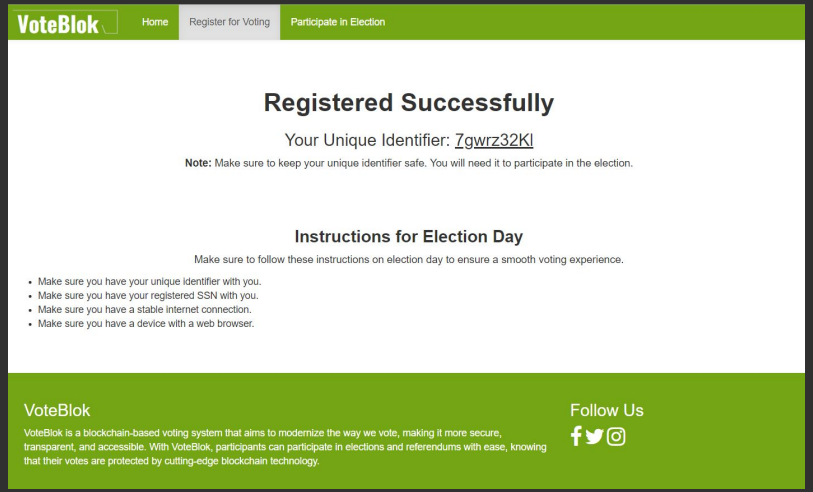
1. Candidate Creation

- The election agency will initialize the smart contract and create candidates
- Will publicly announce the candidates’ blockchain addresses

2. Voter Registration

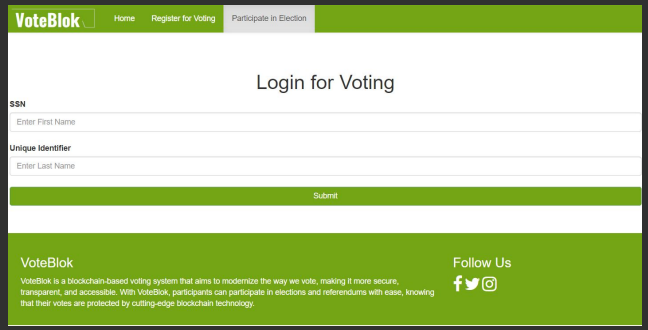
- The voter will register using their ssn and personal information
- A unique identifier will be created and associated with them
- The voters will note this ID and use it for voting

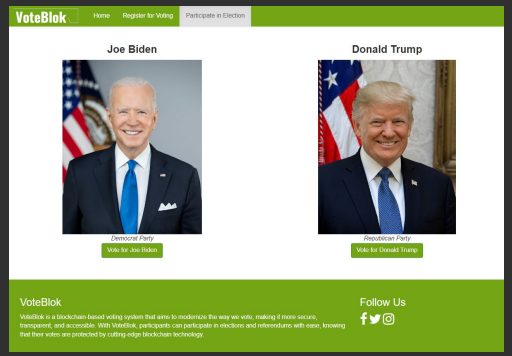


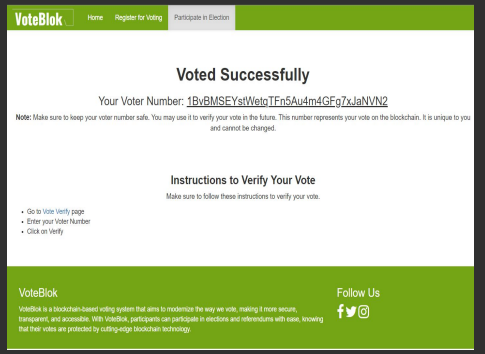


3. Voting

- Voters will login to the system with their ID’s, and will cast a vote
- They will send an API request to receive a random blockchain address
- A transaction with the vote will be sent using this address
- The blockchain address will be shown to the voter for later confirmation

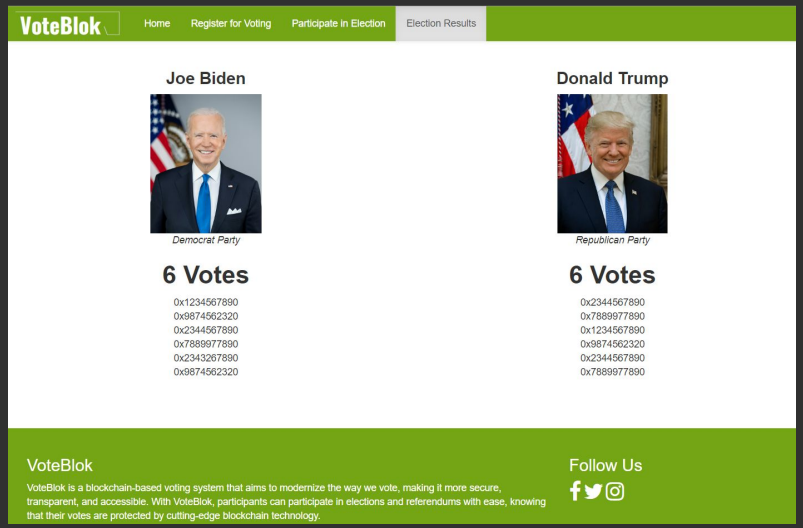






4. Results and Confirmation

- The total vote count for candidates will be released
- The blockchain address of each voter will be listed for each candidate, so that they can confirm their vote has been counter



What we learned

- Blockchain is kinda “meh” for government elections
- It really is hard to trust the government
- Online elections are hard to make safe, as proven by researchers before

VoteBlok

Blockchain-Based Open Source Governmental Election System

MURAD MIKAYILZADE, MERT YAPUCUOGLU, AHMET TURAN BULUT

UNIVERSITY OF OREGON

Introduction

The act of voting lies at the heart of democratic societies, allowing citizens to exercise their right to have a say in the decisions that shape their communities and nations. However, traditional voting systems have long faced challenges related to security, transparency, and accessibility. These shortcomings have led to concerns about voter fraud, tampering, and the overall trustworthiness of election results. In the digital era, leveraging innovative technologies becomes imperative to address these issues and modernize the voting process.

VoteBlok emerges as a transformative solution, harnessing the power of blockchain technology to transform the way we vote. By employing the inherent properties of blockchain - decentralization, immutability, and transparency- VoteBlok strives to establish a secure, and transparent voting system. With VoteBlok, participants can engage in elections and referendums with ease, confident that their votes are protected by cutting-edge cryptographic algorithms and a distributed ledger that cannot be tampered with.

Methodology

In order to provide a safe, untraceable, dupe-proof, and reliable voting system, we had to choose between the available tools and merge them to create all processes of an election. The created election process consists of three parts, and we will examine each one in order down below.

1. Voter Registration
2. Voting
3. Confirmation

Voter Registration

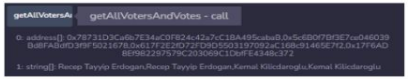
This step is necessary to create a list of eligible voters, and give voters an ID that they will use to login to the voting system. Using this ID, the system will be able to distinguish who can login, and can also keep track if the owner of the ID has already voted. To build this, we will use a simple React / NodeJS website with a connection to a government database, which we will simulate with a FirebaseDB. In the front page, we will take user input including social security number, name, last name, date of birth, address, and phone number, and will confirm the details with a query to the database.

Methodology (cont'd)

If the user is an eligible voter, the system will create a secret identifier that is 9 characters long, contains numbers, letters and is case-sensitive. This secret will be encrypted with SHA-256 and will be kept in the database to confirm login when the voting begins.

Voting

For the temper-proof and reliability purposes of our system, we utilized blockchain to keep track of the votes, the total vote count, and each candidate's total votes. The government will create and deploy a public Ethereum Smart Contract written in Solidity. It will contain structures for candidates and voters, and will have functions that will enable candidate creation and voter creation. Because the owner of the contract, the government, holds the permissions to the contract, they can manage which functions are reachable by the public, but all can view it as well as the blockchain itself. To complement and serve the Contract to public during voting, there will be a React/NodeJS front-end with the Smart Contract integrated with Hardhat. When voters login to the voting page and cast their vote, a blockchain address is created by the front-end and the contract function to create a voter is called with the address. This creates a Voter struct and is stored in the voters mapping, linking the voter's Ethereum address to their struct. However, the struct contains only the vote and nothing personal about the voter, so it is an anonymous vote. As the blockchain address will be discarded after being shown to the voter, there is no way to trace who created which transaction to cast their vote.



How Votes are Kept Along with Their Addresses in the blockchain

Results

Here we will discuss the developed web pages, the voting blockchain, and their usage for a regular election process.

Voter Registration

The idea of this step is mostly to provide a safe way to attach a secret identifier to each voter, and to confirm their eligibility to vote. Here, we present a public website to the voters, link to which is on governmental website. Each voter will sign in with their social security number, and a list of other personal information explained in Methodology. If they are eligible to vote, they will be told so on the website and their secret identifier will be created and provided, which they will be told to note down. The secret identifier will be encrypted and stored in government database to be checked during login when the voting system becomes online.

Registration Page

Registration Success

Voting

Once the voting begins, the link to the voting website will be shared on the government website. The code to this website will be public, as will the logs and all internet activity of its host server. This way any information that will be entered to the website to vote will not be stored by the government to match voters with their votes, and the voters will be able to confirm that it is so. The users will login to the voting panel using their social security number and the secret identifier assigned to them on Voter Registration. The system will check if the encrypted version of the secret identifier is in the database, and if the voter already voted. If not, the voter will be allowed to login to the voting page.

Results (cont'd)

Voting Login

Once on the voting page, the voters will be able to select their candidates, and will press the "Vote" button on the page. Upon pressing the button, thel website will create a one-time blockchain address to the user, and use this address to initiate a transaction including the vote. The server will notify the database that the owner of the secret identifier has voted. Once this is over, the blockchain address will be displayed to the voter, and they will be told to note it down if they want to confirm their vote afterward.

Voting Page

Voting Success

Confirmation

After the voting period ends, the election results will be easily counted by the counter value in the transactions. Additionally, the blockchain addresses and their corresponding vote will be published on a government website. The voter that have noted their address will be able to confirm their vote and make sure it has been safely counted for.

Voting Results