International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13, Issue 4, April-2024, Impact Factor: 8.285
Presented at "ICRETETM-2024", Organized by GSMCOE, Pune, on 22nd - 23rd April 2024

Smartvotex-Empowering Elections with Blockchain

Pratik Jagdale[1], Prajyot Malwade[2], Om Kate[3], Onkar Pathak[4], Sushant Jagtap[5], Pranjali Ghode[6]

[123456]Computer Department, Genba Sopanroa Moze College of Engineering.
Balewadi, Pune, Maharashtra, India

ABSTRACT

The traditional paper ballot framework and commonly utilized electronic voting gadgets can both be substituted with online voting. Other than guaranteeing straightforwardness in vote casting and defending voter privacy, an electronic voting stage must prioritize security and data astuteness. This research advocates for the selection of a blockchain-based electronic voting framework to address certain confinements inalienable in current voting techniques. The paper moreover investigates existing blockchain-based voting systems. The current usage is custom-made for small-scale races conducted in limited settings such as workplaces and meeting rooms. This ponder presents a direct approach for an even handed electronic voting framework that ensures secrecy, resistance to constraint, precision, ease of counting, qualification, fair-mindedness, availability, judgment, and flexibility. It moreover addresses voter confirmation, voter secrecy, vote unquestionable status, and open verifiability, all encouraged by blockchain innovation..

Keywords— Blockchain, E-Voting, Online Voting, Crypto Voting, Hashing

INTRODUCTION

In each vote based system, the assurance of an race may be a matter of national security. The pc security field has for a decade examined the probabilities of electronic choice systems, with the objective of minimizing the cost of getting a national decision, though satisfying and expanding the protection conditions of an decision. From the day break of democratically choosing candidates, the legitimate framework has been upheld pen and paper. Commutation the normal pen and paper topic with a replacement election system is basic to restrain extortion and having the choice method traceable and irrefutable. Electronic choice machines are viewed as flawed, by the assurance community, based totally on physical security contemplations. Anybody with physical access to such machine will sabotage the machine, subsequently moving all votes run up the said machine.

Enter blockchain technology –

A blockchain seem be a dispersed, permanent, undeniable, open record. This unused innovation works through four primary features:

1. The record exists in numerous distinctive areas: no single point of disappointment in the support of the conveyed ledger.
2. There is conveyed administration over joined together countries office will add modern exchanges to the ledger.
3. Any anticipated "new block" to the record should reference the past adaptation of the record, making a changeless chain from wherever the blockchain gets its title, and so anticipating intruding with the judgment of past entries.
4. A majority of the arrange hubs must reach a agreement some time recently a proposed modern square of passages gets to be a changeless portion of the ledger. These mechanical alternatives work through advanced cryptography, giving a security level break even with and/or bigger than any antecedently striking data.

The blockchain innovation is hence thought of by several, together with America, to be the best instrument, to be accustomed produce the unused in vogue law based poll method. This paper assesses the employment of blockchain as a

service to actualize relate degree electronic poll (e-voting) framework. The framework makes the ensuing original contributions.

1. Research existing blockchain systems suited to constructing blockchain fundamentally based e-voting system.
2. Propose a blockchain-based e-voting framework that uses "permissioned blockchain" to modify liquid democracy.

LITERATURE SURVEY

2.1 SURVEY EXISTING SYSTEM

1. Adida, B., Helios (2008). "Web-based open-audit voting.", in Procedures of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Affiliation, 2008.This paper proposes related legitimize an adequate security show and criteria to judge comprehensibility. It also portrays a web vote theme, pretty graspable Popular government, appear that it satisfies the satisfactory security show which it's a parcel of graspable than Lovely shrewd Majority rule government, directly the sole topic that also fulfils the arranged security model.

2. Chamu, D., Essex, A., Carback, R., Clark,J., Popoveniuc, S., Sherman, A. and Vora, P.(2008)."Scantegrity: End-to-end voter-Contiguity- filter voting.", IEEE Security, vol.6, no. 3, pp. 40-46, May 2008.This paper depicts Contiguity that minimally impacts decision methods and is the to begin with autonomous E2E confirmation instrument that preserves optical filter as the fundamental voting framework and doesn't meddled with a manual recount.

3. Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A reasonable and strong voting framework by broadcast.",5th Worldwide Conference on E-voting, 2012.This paper proposes a recuperation circular to empower the election result to be declared if voters prematurely end and also included a commitment circular to guarantee fairness. In expansion, it too given a computational security confirmation of poll secrecy.

4. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D.,Eakin, B., Kortum, P., McBurnett, N., Pereira, O.,Stark, P. B., Wallach, D. S., Fisher, G., Montoya,J., Parker, M. and Winn, M. (2013)."Star-vote: A secure, straightforward, auditable, and dependable voting system.", in 2013 Electronic Voting Innovation Workshop/Workshop on Dependable Elections(EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

This paper portrays the STAR-Vote plan, that may ideally be the next-generation constituent framework for Travis Province and perhaps elsewhere. Recent major specialized challenges relating to e-voting systems grasp, in any case not confined to secure computerized personality administration. Any potential citizen should tore enrolled to the discretionary framework some time recently the elections. Their information should to be in an exceptionally carefully processable organize. Other than, their personality information should to be unbroken individual in any including data. Old E-voting framework might confront taking after problems:

• Anonymous vote-casting.
• Individualized poll processes.
• Vote casting unquestionable status by (and as it were by) the voter.
• High initial setup costs.
• Expanding security problems.
• Need of straightforwardness and trust.
• Voting delays or wasteful aspects related to remote/absentee voting.

2.2 IMPEDIMENTS OF EXISTING FRAMEWORK OR RESEARCH GAP

Recent major specialized challenges relating to e-voting systems epitomize, be that as it may not limited to secure computerized personality administration. Any potential citizen should to are enrolled to the appointive framework some time recently the elections. Their information should to be amid a carefully processable arrange. Other than, their personality information should to be unbroken on-public in any including data. Old E-voting system might confront taking after problems:

• **Anonymous vote-casting:** Each vote may or may not contain any choice per candidate, ought to be anonymous to everybody counting the framework chairmen, after the vote is submitted through the system.

• Individualized poll forms: How a vote is portrayed inside the including net applications or databases continues to be AN open dialog. while a straightforward content message is that the most exceedingly bad arrange, a hashed tokenism want to offer lack of definition and judgment. In the meantime, the vote should to be non-reputable, that can't be reinforced by the token resolution.

• **Vote casting unquestionable status by (and as it were by) the voter:** The voter should to be prepared to see and confirm his/her own vote, when he/she submitted the vote. this is often vital to realize so as to hinder, or a least of two notes, any potential pernicious action. This counter live, except for giving recommends that of non-repudiation, can beyond any doubt boost the sensation of believe of the voters. These issues zone unit mostly self-addressed in a few recent applications. However, recommends that of e-voting is presently in utilize in numerous nations together with Brazil, kaipen, and Republic of Estonia. Republic of Estonia ought to be assessed something else than the others, since they supply a full e-voting determination that's, said to be, equivalent of antiquated paper-based elections.

• **High beginning setup costs:** In spite of the fact that supporting and keeping up on-line choice frameworks is way cheaper than antiquated races, beginning organizations may be pricy, especially for businesses.

• **Expanding security :** Be equivalent assaults cause an excellent risk to the common open surveys. nobody would settle for the duty if relate degree hacking attempt succeeds all through a decision. The DDoS attacks are recorded and generally not the case within the races. The citizen keenness commission of the us gave a sworn statement concerning the state of the elections within the North American nation as of late. Appropriately; Ronald Rivest expresses that "hackers have myriad ways in which of assaultive choose machines". As relate degree case; barcodes on votes and smartphones in choose areas may be utilized in the hacking method. Apple express that we tend to mustn't ignore the real reality that computers are hackable, and moreover the evidences will basically be erased. Double-voting or voters from the inverse locales moreover are a few common issues.

To moderate these dangers, program components which promise the taking after ought to be deployed:
1. Anticipation of prove deletion
2. Straightforwardness with privacy.

• **Need of straightforwardness and believe:** How can individuals without a doubt believe the comes about, when everything is done online? Perceptual issues cannot be ignored.

• **Voting delays or wasteful aspects related to remote voting:** Timing is exceptionally imperative in voting schemes; specialized capabilities and the foundations ought to be dependable and run at the highest possible execution to let farther voting bisynchronous.

2.2.1 Problem Statement and objectives

Our objective is to unravel the issues of advanced voting by using blockchain technology. Blockchain empowered e-voting could decrease voter extortion and increment voter access.

2.3 OBJECTIVES

Thus, the voting framework that is therefore conceived must satisfy the taking after requirements:

1. The race framework must be straightforwardly irrefutable and transparent.
2. The race framework must guarantee that the vote cast by the voter has been recorded.
3. As it where qualified voters must be permitted to vote.
4. The decision framework ought to be tamper-proof.
5. No power-hungry organization must be able to control and fix the decision process. Using a Blockchain, the most critical requirements are fulfilled:

• **Verification:** As it where enlisted voters will be allowed to vote.
• **Namelessness:** The framework avoids any interaction between the votes casted by the voters and their identities.
• **Exactness:** Votes once cast are forever recorded and cannot be altered or changed beneath any circumstances.
• **Unquestionable status:** The framework will be unquestionable such that the number of votes is accounted for.

PROPOSED SYSTEM

The simple rationalization may be a 'chain' of blocks. A block is relate degree mass set of data. information square degree collected and method to suit in an exceedingly block through a process known as mining. each square may be known utilizing a science hash (also referred to as a computerized unique finger impression). The block formed can contain a hash of the past square, so blocks will kind a sequence from the essential square ever (known since the Genesis Block) to the formed block. amid this method, all the data may be associated by means of a associated list structure.

3.1 ANALYSIS/FRAMEWORK/ALGORITHM

Working:

• The SHA-512 calculation takes an input of any random length and produces an yield of a settled length(512 bits).
• In the case of SHA-512 calculation no matter how big or small is the input, the yield is of settled length(512 bits).

A cryptographic hash work has the taking after properties:

1. Deterministic: This implies that no matter how many times we enter the same input we will get same result.

2. Speedy Computation: This implies that the result is generated rapidly and this leads to an increment in the framework efficacy.

3. Pre-Image resistance: Suppose we are rolling a dot(1-6) and instep of getting a particular number we get the hash value. Now we calculate the hash value of each number and at that point compare it with the Result . And for a bigger information sets it is conceivable to break pre-Image resistance by brute drive strategy and this takes as well long that it does not matter.

4. Small changes in Input alter the entirety Output: A minor alter in the input essentially changes the entirety output.

5. Collision Resistant: Every input will have a unique hash value.

6. Puzzle friendly: The combination of two values gives the hash esteem of unused variable.

The require of hashing in blockchain:

- The blockchain is a grouping of squares that contain data.
- Each block has a hash pointer that contains previous block's data.
- So if a programmer tries to assault a specific piece, the changes will be reflected to the whole chain of blocks.
- Subsequently, the blockchain concept is so revolutionary**.**

3.2 DETAILS OF HARDWARE AND SOFTWARE

3.2.1 Software Requirements

• **OS:** Windows 10.
• **Framework:** Visual Studio.
• **Server:** Localhost.

3.2.2 Hardware Requirements

• **Processor:** Intel Quad core 1.5 GHZ Processor or above.
• **HD:** Minimum 10 GB of HD.
• **RAM:** Minimum 8 GB of RAM.

3.3 DESIGN DETAILS

Our voting system architecture is a sophisticated blend of Django, a powerful Python web framework, and blockchain technology, augmented with HTML, CSS, and JavaScript for the frontend interface.

Django: This robust framework forms the backbone of our web application, providing essential features like user authentication, session management, and URL routing. Within our system, Django seamlessly handles user authentication, facilitates email communication for OTP verification, and orchestrates database interactions for storing and retrieving voting data.

Python: Serving as the primary programming language for the backend logic, Python empowers our system with its simplicity and readability. It enables rapid development and maintenance of the complex voting system functionalities, such as vote validation, blockchain integration, and cryptographic operations.

Blockchain Technology: At the heart of our architecture lies blockchain technology, which revolutionizes the voting process by ensuring transparency, immutability, and security. Leveraging blockchain, our system guarantees tamper-proof recording of votes, transparent verification, and decentralized consensus mechanisms. Through smart contracts and cryptographic hashing, the integrity of the voting process is upheld, offering users trust and confidence in the outcome.

HTML, CSS, and JavaScript: Frontend development is facilitated by HTML, CSS, and JavaScript, which together create an intuitive and interactive user interface. HTML structures the content, CSS styles the layout, and JavaScript adds dynamic behavior to enhance user experience. This frontend stack enables voters to seamlessly interact with the voting system, casting their votes securely and conveniently.

Integration: Django harmoniously integrates frontend and backend components, providing a cohesive user experience. HTML templates are rendered dynamically by Django, allowing for the seamless incorporation of backend data into the frontend interface. JavaScript enhances interactivity, enabling real-time updates and validation of user inputs. Through this integrated approach, our voting system delivers a smooth and responsive user experience across all devices.

Security: security is paramount in our architecture, with django's built-in security features complemented by blockchain's cryptographic safeguards. user authentication, data encryption, and secure communication protocols are rigorously implemented to protect sensitive information and ensure the integrity of the voting process.

By leveraging the strengths of Django, Python, blockchain technology, and frontend technologies like HTML, CSS, and JavaScript, our voting system sets a new standard for transparency, security, and user engagement in the democratic process

3.3.1 DETAILED DESIGN

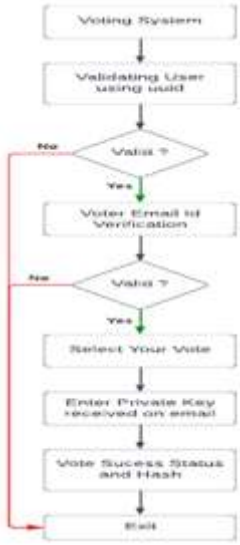

Fig 1. Flow chart of the system

Upon visiting the Smartvotex website, users are prompted to authenticate their identity by entering their Aadhar number, a pre-requisite for registration administered by the site's administrators. Upon successful verification, users gain access to their personal profile, where an additional layer of security is enforced through email verification. An OTP (one-time password) is dispatched to the registered email address, serving as a verification mechanism. Once the email verification process is completed, users are granted the privilege to exercise their voting rights.

To proceed with casting their vote, users are required to furnish a private key, which is securely dispatched to their registered email address. This private key serves as a unique identifier and ensures the integrity of the voting process. Upon successfully submitting their vote, users are presented with a digitally generated hash for their ballot, along with a digital signature, affirming the authenticity and integrity of their vote.

3.4 METHODOLOGY

Sequence diagram of the project -

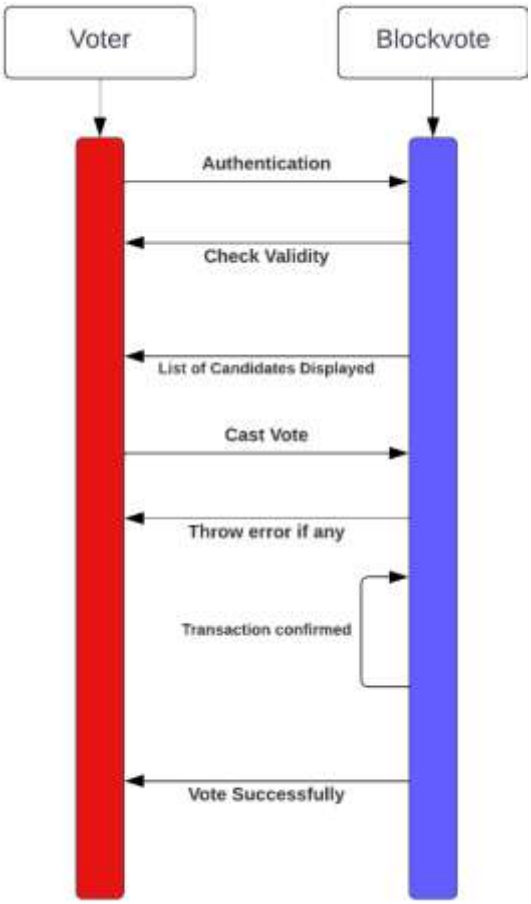

Fig 2. Sequence flow of the project

RESULTS

1. Smartvotex home page

Fig 2. Home Page

2. Voter Information after Login With Aadhar

Fig 3 . User Information

3. Voter Email Verification

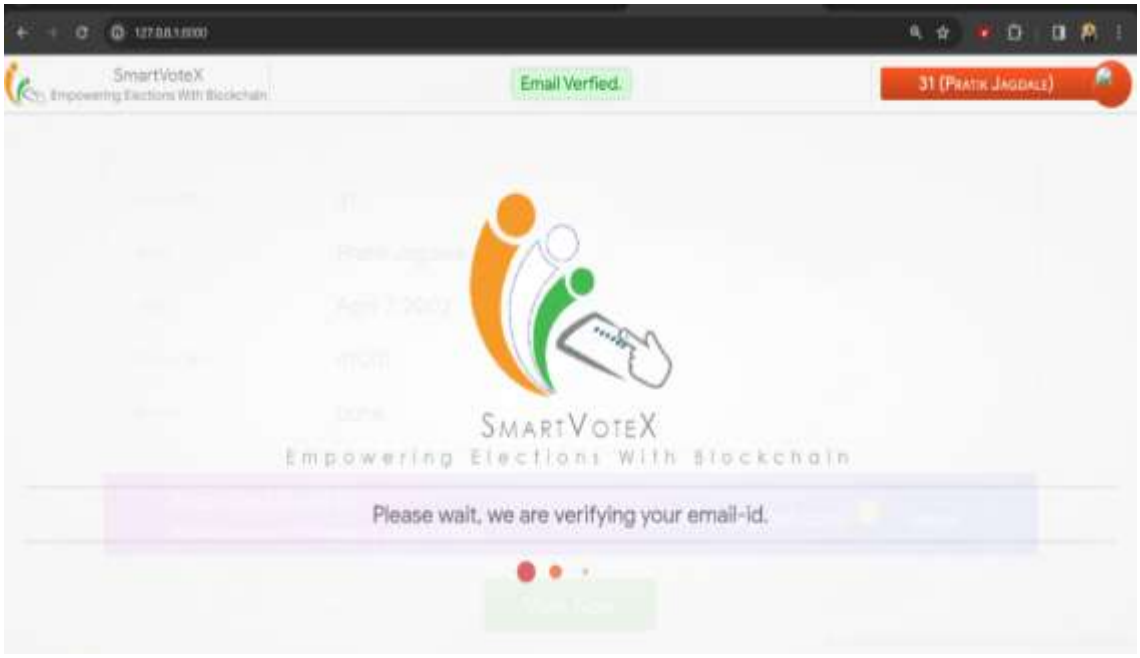

Fig 4. Email Verification

4. Selection Party to Give Vote

Fig 5. selection of vote

5. Verifying private key send on email

Fig 6. Verify Private Key

6. Vote Conformation with hash values

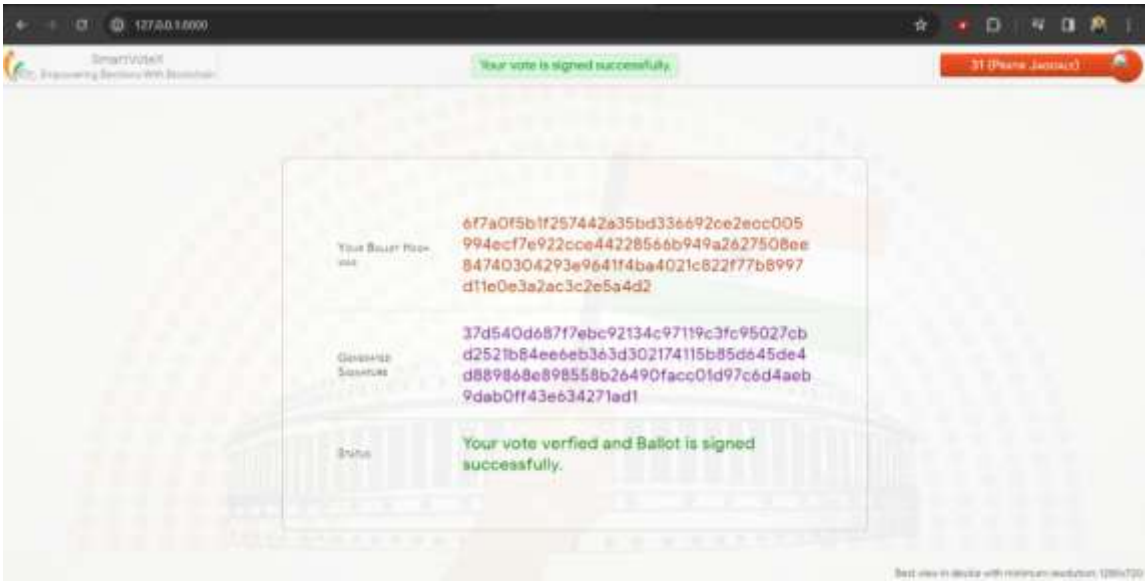

Fig 7. conformation hash of vote

CONCLUSION

The integration of blockchain technology, coupled with cryptography, offers a transformative result to the challenges anguishing traditional voting systems. By using the decentralized nature of blockchain and the cryptographic principles of security and invariability, our voting system ensures translucency, integrity, and responsibility throughout the electoral process. Through the relinquishment of blockchain, we've achieved a distributed tally system that records each vote in a tamper- evidence and transparent manner. This not only mitigates the threat of fraud and manipulation but also fosters lesser confidence among stakeholders in the electoral process.

Likewise, cryptography plays a vital part in securing the authenticity and sequestration of each vote. exercising cryptographic mincing algorithms ensures that each vote is uniquely linked and cryptographically secured, securing it

against unauthorized access or tampering.While our system doesn't employ smart contracts, the application of blockchain and cryptography alone significantly enhances the security and trustability of the voting process. By decentralizing the storehouse and verification of votes, we exclude single points of failure and reduce the liability of electoral malpractice.In substance, our approach to voting using blockchain and cryptography lays the foundation for a more popular, transparent, and inclusive electoral system. As we continue to introduce and upgrade these technologies, we move closer towards realizing a future where every vote counts and every voice is heard

REFERENCES

[1] TANIKELLA SAI CHARAN, SRINANDA PENTAPATI, Mrs. R. PREMA "A Review Paper on E-Voting Using Blockchain Technology", International Research Journal of Engineering and Technology, 2021.
[2] Adida, B., Helios (2008). "Web-based open-audit voting." in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008.
[3] Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, and Prathmesh Potdar "Blockchain technology based e-voting system." ITM Web of Conferences 32, 03001 (2020) ICACC-2020
[4] Ali Benabdallah, Antoine Audras, Louis Coudert, Nour El Madhoun, and Mohamad Badra "Analysis of Blockchain Solutions for E- Voting: A Systematic Literature Review" IEEE Access, IEEE, 2022, 10, pp.70746-70759,ff10.1109/access.2022.3187688ff. ffhal- 03717773ff
[5] Dalia Khader, Ben Smyth, Peter Y. A. Ryan, and Feng Hao "A Fair and Robust Voting System by Broadcast" 5th International Conference on E-voting, 2012.
[6] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-veriable optical- scan voting.", IEEE Security Privacy, vol.6, no. 3, pp. 40-46, May 2008