E-VOTING SYSTEM USING BLOCKCHAIN WITH CNN BASED FACE RECOGNITION

Thummala Pavan Kumar , Arumulla Ajay , Alla Naga Teja , Pandi Chinna Govindu , Diyyala Venkat Ananth Sai Badri

School of Computer Science and Engineering

Lovely Professional University. Phagwara, Punjab, India

ABSTRACT: In this research we are focusing on Blockchain E-Voting. Election could be a important event during a trendy democracy however massive sections of society round the world don't trust their election system that is major concern for the democracy. Even the world's largest democracies like Republic of India, us, and Japan still suffer from a blemished legal system. Vote rigging, hacking of the EVM (Electronic vote machine), election manipulation, and booth capturing square measure the key problems within the current electoral system. during this system, we tend to square measure work the problems, the problems within the election vote systems and attempting to propose the E-voting model which might resolve these issues. The system can highlight a number of the popular blockchain frameworks that provide blockchain as a service and associated electronic E-voting system that is predicated on blockchain that addresses all limitations severally, it additionally preserve participant's obscurity whereas still being hospitable public examination. Building Associate in nursing electronic electoral system that satisfies the legal necessities of legislators has been a challenge for an extended time. Distributed ledger technologies are Associate in nursing exciting technological advancement within the info technology world. Blockchain technologies supply Associate in nursing infinite vary of applications cashing in on sharing economies. Blockchain could be a unquiet technology of current era and guarantees to enhance the resilience of e-voting systems. this technique presents a shot to leverage edges of blockchain like cryptological foundations and transparency to attain an efficient theme for e-voting.

Keywords—Blockchain, Electronic Voting System and E-voting.

INTRODUCTION

In each democracy, the protection of AN election may be a matter of national security. the pc security field has for a decade studied the probabilities of electronic choice systems, with the goal of minimizing the price of getting a national election, whereas fulfilling ANd increasing the protection conditions of an election. From the dawn of democratically electing candidates, the legal system has been supported pen and paper. commutation the normal pen and paper theme with a replacement election system is essential to limit fraud and having the choice method traceable and verifiable. Electronic choice machines are viewed as blemished, by the protection community, based totally on physical security considerations. Anyone with physical access to such machine will sabotage the machine, thereby moving all votes run up the said machine. Enter blockchain technology.

FEATURES

A blockchain could be a distributed, immutable, incontrovertible, public ledger. This new technology works through four main features:

1. The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

2. There is distributed management over United Nations agency will append new transactions to the ledger.

3. Any projected “new block” to the ledger should reference the previous version of the ledger, making a changeless chain from wherever the blockchain gets its name, and so preventing meddling with the integrity of previous entries.

4. A majority of the network nodes must reach a consensus before a voting new block of entries becomes a permanent part of the ledger.

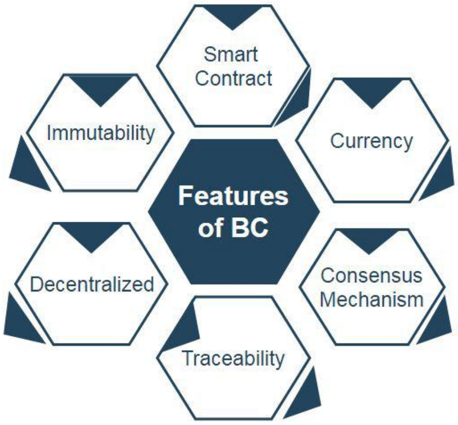

Fig.1: Blockchain features

These technological options operate through advanced cryptography, providing a security level equal and/or bigger than any antecedently notable information. The blockchain technology is thus thought of by several, together with America, to be the best tool, to be accustomed produce the new fashionable democratic ballot method.

SCOPE

The following improvements can be made to the system,

- Adding Aadhar number verification system.

- Linking application with Government voting system data.

- Making the system more secure.

- Enhnacing the Graphical User Interface(GUI) of the application.

- Local languages can be included which will play a vital role for people living in rural areas as well as uneducated people.

- A Candidate’s earlier social work and candidate qualification’s can be added for a voter to have better choice.

- Also, adding suggestion system for voters that enables the public to give suggestions to the current winner.

- A complaint system can be included, that allows the people to file complaint against a candidate.

LITERATURE SURVEY

Web-based open-audit voting, 2008:

This paper proposes associated justify an adequate security model and criteria to judge comprehensibility. It additionally describe a web ballot theme, Pretty graspable Democracy, show that it satisfies the adequate security model which it's a lot of graspable than Pretty smart Democracy, presently the sole theme that additionally satisfies the planned security model. Voting with cryptographic auditing, sometimes called open-audit voting, has remained, for the most part, a theoretical endeavor. In spite of dozens of fascinating protocols and recent ground-breaking advances in the field, there exist only a handful of specialized implementations that few people have experienced directly. As a result, the benefits of cryptographically audited elections have remained elusive.

Scantegrity: End-to-end voter-veriable optical- scan voting, 2008:

This paper describes Scantegrity that minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn't interfere with a manual recount. Voter confidence in the US electoral process is eroding as a steady stream of reports continue to expose fundamental security flaws in certified electronic voting machines. Similar voting technology is used outside of the US, and resistance to electronic voting has spread to other democracies. Although proposals such as stricter design standards, more open systems (preferably open source), and independent verification methods (such as paper audit trails) are improvements, they don't go far enough. In any voting system, with or without an electronic component, the core security problem is chain of custody. An attacker who breaks chain of custody could stuff the ballot box, delete or switch votes, or add votes to contests that the voter left empty. Whether the attacker accomplishes this by inserting malicious code or altering paper ballots, such attacks go undetected even with a manual vote recount.

A fair and robust voting system by broadcast, 2012:

Hao, Ryan & Zieliski (2010) propose a two-round decentralized voting protocol that is efficient in terms of rounds, computation, and bandwidth. However, the protocol has two drawbacks. First, if some voters abort then the election result cannot be announced, that is, the protocol is not robust. Secondly, the last voter can learn the election result before voting, that is, the protocol is not fair. Both drawbacks are typical of other decentralized e-voting protocols. This paper proposes a recovery round to enable the election result to be announced if voters abort and also added a commitment round to ensure fairness. In addition, it also provided a computational security proof of ballot secrecy.

Star-vote: A secure, transparent, auditable, and reliable voting system, 2013.

This paper describes the STAR-Vote design, that may preferably be the next-generation electoral system for Travis County and maybe elsewhere. STAR-Vote is a collaboration between a number of academics and the Travis County (Austin), Texas elections office, which currently uses a DRE voting system and previously used an optical scan voting system. STAR-Vote represents a rare opportunity for a variety of sophisticated technologies, such as end-to-end cryptography and risk limiting audits, to be designed into a new voting system, from scratch, with a variety of real world constraints, such as election-day vote centers that must support thousands of ballot styles and run all day in the event of a power failure.

Limitations of Existing system:

Recent major technical challenges relating to e-voting systems embrace, however not restricted to secure digital identity management. Any potential citizen ought to are registered to the electoral system before the elections. Their data ought to be in a very digitally processable format. Besides, their identity data ought to be unbroken personal in any involving information. ancient E-voting system could face following problems:

- Anonymous vote-casting.
- Individualized ballot processes.
- Ballot casting verifiability by (and only by) the voter.
- High initial setup costs.
- Increasing security problems.
- Lack of transparency and trust.
- Voting delays or inefficiencies related to remote/absentee voting.

Anonymous vote-casting:

Each vote may or may not contain any choice per candidate, should be anonymous to everyone including the system administrators, after the vote is submitted through the system.

Individualized ballot processes:

How a vote are depicted within the involving net applications or databases continues to be AN open discussion. whereas a transparent text message is that the worst plan, a hashed token is wont to offer obscurity and integrity. Meanwhile, the vote ought to be non-reputable, that can't be bonded by the token resolution.

Ballot casting verifiability by (and only by) the voter:

The elector ought to be ready to see and verify his/her own vote, when he/she submitted the vote. this is often vital to realize so as to forestall, or a minimum of to note, any potential malicious activity. This counter live, except for providing suggests that of non-repudiation, can sure boost the sensation of trust of the voters. These issues area unit partly self-addressed in some recent applications. Yet, suggests that of e-voting is presently in use in many countries together with Brazil, uk, Japan, and Republic of Estonia. Republic of Estonia ought to be evaluated otherwise than the others, since they supply a full e-voting resolution that's, said to be, equivalent of ancient paper-based elections.

High initial setup costs:

Though sustaining and maintaining on-line selection systems is way cheaper than ancient elections, initial deployments could be pricy, particularly for businesses.

Increasing security problems:

Cyber attacks cause an excellent threat to the general public polls. nobody would settle for the responsibility if associate degreey hacking try succeeds throughout an election. The DDoS attacks ar documented and largely not the case within the elections. The citizen integrity commission of the u. s. gave an affidavit concerning the state of the elections within the North American country recently. Accordingly; Ronald Rivest explicit that “hackers have myriad ways in which of assaultive pick machines”. As associate degree example; barcodes on ballots and smartphones in pick locations may be utilized in the hacking method. Apple explicit that we tend to mustn’t ignore the actual fact that computers ar hackable, and also the evidences will simply be deleted. Double-voting or voters from the opposite regions also are some common issues.[8]

To mitigate these threats, software mechanisms which promise the following should be deployed:

1. Prevention of evidence deletion.

2. Transparency with privacy.

Lack of transparency and trust:

How can people surely trust the results, when everything is done online? Perceptual problems cannot be ignored.

Voting delays or inefficiencies related to remote voting:

Timing is very important in voting schemes; technical capabilities and the infrastructures should be reliable and run at the highest possible performance to let remote voting be synchronous.[5]

E-VOTING BACHGROUND & REQUIREMENTS

Electronic voting has been an area of research focus for many years by using computing machines and equipment for casting votes and producing high quality and precise results in accordance with the sentiments of the participating voters. Various attempts have been adopted in practice to support election process. Initially computer counting system allowed the voter to cast vote on papers. Later on, those cards went through the process of scanning and tallying at every polling cell on a central server (Kadam et al, 2015; Rockwell, 2017; Hao et al, 2010).

Direct Recording Electronic (DRE) voting systems were put in place later on which were admired and acknowledged greatly by the voters in-spite of the resistance from computer scientists. If the voting system is well understood by the voters, the system’s usability can be increased remarkably. DRE systems in particular have gathered a lot of successes in bringing the voters to use this technology. These systems work more or less in the same way as any conventional election system does. In the case of DRE, a voter begins his journey by going to their polling place and get their token to vote where he utilizes his token at the voting terminal to vote for his candidate. When the candidate selection procedure is completed, DRE systems present the final selection to the voter before actually casting it (in case if the voter wants to change his opinion) and after the final selection, the ballot casting is completed (Multichain, 2017; Dalia et al, 2012).

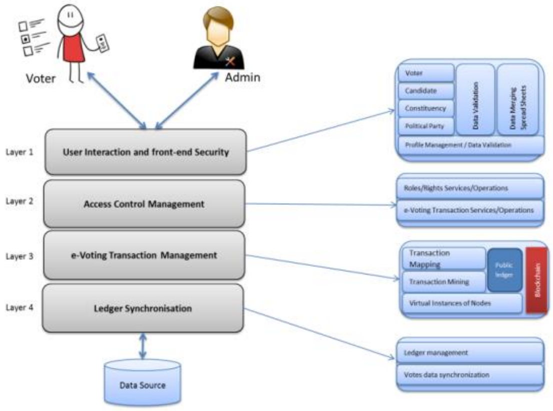
Voter
Admin
Layer 1
User Interaction and front-end Security
Layer 2
Access Control Management
Layer 3
e-Voting Transaction Management
Layer 4
Ledger Synchronisation
Data Source
Voter
Candidate
Constituency
Political Party
Data Validation
Data Merging Spread Sheets
Profile Management / Data Validation
Roles/Rights Services/Operations
e-Voting Transaction Services/Operations
Transaction Mapping
Transaction Mining
Public ledger
Virtual Instances of Nodes
Blockchain
Ledger management
Votes data synchronization

Fig.2: Direct Recording Electronic (DRE) voting systems

More recently, distributed ledger technologies such as blockchain have been used to achieve e-voting systems primarily due to their advantages in terms of end-to-end verifiability. With properties such as anonymity, privacy protection and non-repudiation, blockchain is a very attractive alternative to contemporary e-voting systems. The research presented in this paper also attempts to leverage these properties of blockchain to achieve an efficient e-voting system. A detailed analysis of such systems is presented in the next section along with the identification of comparison with these approaches.

THE VOTING PROCESS

We now describe a typical interaction of a user with the voting scheme based on our current implementation of the system. Typically, a voter logs into the system by providing his/her thumb impression. If the match is found, the voter is then presented with a list of available candidates with the option to cast vote against them. On the contrary, if the match is unsuccessful, any further access would be denied. This function is achieved using appropriate implementation of the authentication mechanism (fingerprinting in this case) and predefined role based access control management. Furthermore, it is also envisioned that a voter is assigned to their specific constituency and this information is used to develop the list of candidates that a voter can vote for. The assignment of voter to a constituency is rendered an offline process and therefore out of scope of this research.

After a successful vote-cast, it is mined by multiple miners for validation following which valid and verified votes are added into public ledger. The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique thumbprint, which is matched at the beginning of every voting attempt to prevent double voting. A transaction is generated as soon as the vote is mined by the miners which is unique for each vote. If the vote is found malicious it is rejected by miners.

After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

ANALYSIS

The simple rationalization could be a 'chain' of blocks. A block is associate degree mass set of information. knowledge square measure collected and methoded to suit in an exceedingly block through a process known as mining. every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will kind a sequence from the primary block ever (known because the Genesis Block) to the shaped block. during this method, all the information may be connected via a connected list structure.

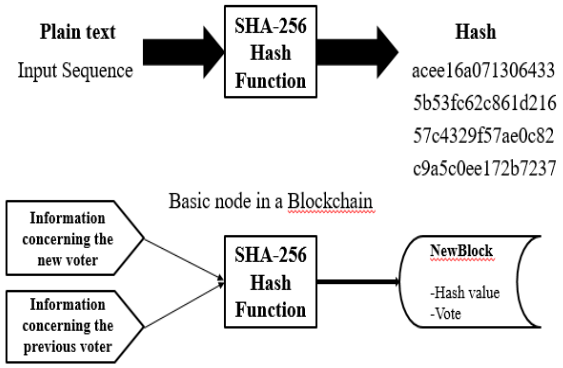

Fig.3: SHa algorithm

STEPS:

1. The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length(256 bits).
2. In the case of SHA-256 algorithm no matter how big or small is the input, the output is of fixed length(256 bits).

The blockchain is a sequence of blocks that contain data. Each block has a hash pointer that contains previous block's data. So if a hacker tries to attack a particular block, the changes will be reflected to the entire chain of blocks. Therefore, the blockchain concept is so revolutionary.

A cryptographic hash function has the following properties:

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

2. Quick Computation: This means that the result is generated quickly and this leads to an increase in the system efficiency.

3. Pre-Image resistance: Suppose we are rolling a dot(1-6) and instead of getting a specific number we get the hash value. Now we calculate the hash value of each number and then compare it with the result. And for a larger data sets it is possible to break pre-Image resistance by brute force method and this takes too long that it does not matter.

4. Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.

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

6. Puzzle friendly: The combination of two values gives the hash value of new variable.

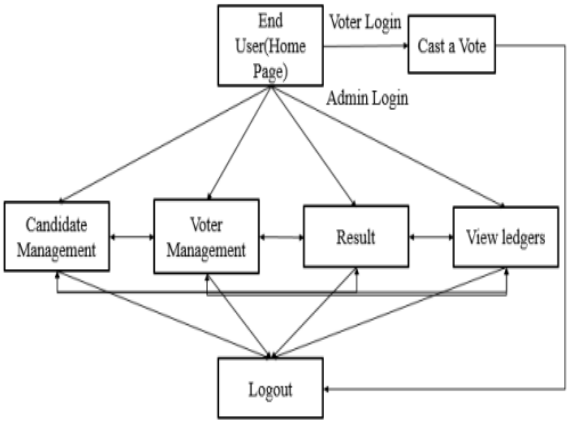

Fig.4: Overview of E-voting

TABLE.1: Result calculated using e-voting system

No of voters	Correct verification	Correct voting count	Accuracy
3	3	3	100%
5	5	5	100%
10	10	10	100%
30	30	30	100%

CONCLUSION

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e-voting. The transparency of the block-chain allows additional auditing and understanding of elections. These attributes square measure a number of the wants of a legal system. These characteristics come back from redistributed network, and may bring additional democratic processes to elections, particularly to direct election systems. For e-voting to become additional open, clear, and severally auditable, a possible answer would be base it on blockchain technology.

The research of this work, we are focused at improving the resistance of blockchain technology to 'double spending' problem which will translate as 'double voting' for e-voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction however successful demonstration of such events have been achieve which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end-to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure.

REFERENCES

[1] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting,"IEEE Software,vol. 35, pp. 95-99, jul 2018.

[2] M. Pawlak, J. Guziur, and A. Poniszewska-Mara nda, "Voting Processwith Blockchain Technology: Auditable Blockchain Voting System," inLecture Notes on Data Engineering and Communications Technologies,pp. 233-244, Springer, Cham, 2019.

[3] B. Singhal, G. Dhameja, and P. S. Panda, "How Blockchain Works," inBeginning Blockchain, pp. 31-148, Berkeley, CA: Apress, 2018.

[4] Agora, "Agora Whitepaper," 2018.

[5] R. Perper, " Sierra Leone is the first country to use blockchain duringan election - Business Insider," 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," tech.rep., 2008.

[7] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger,"Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

[8] S. Landers, "Netvote: A Decentralized Voting Platform - Netvote ProjectMedium," 2018.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract forBoardroom Voting with Maximum Voter Privacy," inLecture Notes inComputer Science, ch. FCDS, pp. 357-375, Springer, Cham, 2017.

[10] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard)LWE,"SIAM Journal on Computing, vol. 43,pp. 831-871, jan 2014.

[11] O. Goldreich and Y. Oren, "Definitions and properties of zeroknowledgeproof systems,"Journal of Cryptology, vol. 7, no. 1, pp. 1-32, 1994.

[12] Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). "A fair and robust voting system." by broadcast, 5th International Conference on E-voting, 2012.

[13] 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, pp. 335348.

[14] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). “Scantegrity: End-to-end voter-veriable opticalscan voting.” , IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[15] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). “Bingo voting: Secure and coercion- free voting using a trusted random number generator.”, in Proceedings of the 1st International Conference on Evoting and Identity, ser. VOTE-ID’07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.