Retraction

Retraction: A Secure Digital E-Voting Using Blockchain Technology (J. Phys.: Conf. Ser. 1916 012197)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
A Secure Digital E-Voting Using Blockchain Technology

Geetha S K1,2, Sathya S2, Sakthi Sree T3
1Assistant Professor, Department of CSE, KPR Institute of Engineering and Technology, Coimbatore
2Assistant Professor, Department of CSE, Hindusthan College of Engineering and Technology, Coimbatore
3Assistant Professor, Department of IT, Hindusthan College of Engineering and Technology, Coimbatore
1geethu.cbe@gmail.com, 2sathyasuriyanme@gmail.com, 3sakthisree@gmail.com

Abstract. In digital electronic voting security is always the biggest anxiety. In existing system, the EVM system used, when compare to the conventional paper ballot system EVM reduces the time for casting vote and result announcement, but still having many issues there is the risk that the election authorities can able to change or remove the vote therefore chances for violating its secrecy. The entire system may rigged by any third party.Blockchain technology provide secure electronic voting platform, which is a decentralized, peer-to-peer transaction ledger enables every vote that is casted will be consider as an individual transaction which creates transparent and secure environment for elections, where the users will be able to cast their votes only once and will be able to view the total votes casted in real time without having the permission to edit the same after election gets over. These votes will be counted and the results will then be announced. This work achieves by solving the issues of digital voting systems and a mechanism to boost the number of voters and their trust in the electoral process.

Keywords: Digital Voting System, Blockchain, Peer-to-Peer transaction, Hashing

1. Introduction
Security of election is biggest concern for every country. Election plays an important role in such a huge democratic country like India where the leader is elected by resident. Elections keep a fair nation functioning, as they give individuals the option to choose their own government. So the election must be a free and fair process. Electronic voting machine has already been developed and widely used in many developed countries. But during the election time, verification process takes a lot more time and there is possible to occur counterfeit vote.

Electoral systems give power to the citizens of a country to select parliament members of their choice. In India, two types voting of method used. The traditional method is secret ballot paper; In this method, printed vote sheets are submitted to various election booths of country at least two days before the election. Voter’s mark their vote and once after election process over vote will be preserved in sealed ballot boxes and the ballot boxes opened in front of all the legitimate members of the booth and counting will be started manually. Once counting process over the counted information is submitted to centralized election team with bags of papers votes.
The election authority compiles the results and publishes the winners name through communication media. This is useful when the entire process is transparent way. Though there are some pitfalls to this system. The entire process requires huge money, longer time to complete the voting process; there are some changes fraudulent practices by election authorities.

The second voting method is Electronic voting machine (EVM) which is in use since 2003. This is alternate method for paper based voting system. Electronic voting machine viewed as weak scheme by the security community. The above said machine primarily malfunctioning based on physical security concerns. The problem of such machine is any unauthorized can try to disrupt the machine, possibility of affecting all votes cast by the voter’s.

The novel alternate method for EVM is online voting (E-voting / i-voting) basically web based voting system useful to carry out the election process skillfully and without threat. The main advantage of the system the citizens need not to go to their concern native to poll their vote. There is no polling booth exist in the novel idea. With the help their handheld electronic device like personal computer, mobile phone they can cast their votes within fraction of seconds.

For i-voting all the information of voters need to be stored and maintained in a database well ahead. The election conducting authority can collect the information of voters by getting filled e-forms.

Once registration process over, the voter is identify with the unique identity number. The number is useful in further election process.

In case if the user given wrong / invalid details, then the person denied to vote. After the successful completion of registration, a link will share to voter’s E-mail IDs. Activation of voter account can be done through by clicking link. User account for voting permitted only when the user clicks the link. Voting option only enabled for the voters on Election Day.

On voting day when the user login, one time password (OTP) generated for the voter which has to be entered by the electors for casting their vote. OTP will destroyed once the voters cast their vote. Due to this unwanted manipulation can be avoided during the vote casting by the voter. Acceptance of the vote will be sent to the ballotor on their registered E-Mail ID’s. User can ensure their vote registration by seeing the acknowledgment.

The main attractive advantage of digital voting system is voters need not to wait in a queue they can cast their vote in their free time therefore congestion is reduced. Digital voting also reduces errors of vote counting.

The disadvantage of online voting is security. Many possible cyber-attacks from external or even from internal actors; the actors may manipulate the votes. Other major attack possible is Denial of service attack which preventing citizens from casting their vote. Sometimes due to errors or malware on voter’s devices may affect the vote cast. In such case voter’s need to be updates their software or browsers.

To overcome all the above said issues a blockchain is alternate approach. A blockchain is immutable distributed ledger, which is incontrovertible public ledger. In blockchain technology ledger maintained usually in various different locations. The technology has four main features.

i) Single point of failure can be avoided because here the ledger normally maintained in distributed fashion.

ii) Anyone in the blockchain network append new transactions to ledger due to its distributed control.
iii) Newly recommended block need to refer the previous version of the ledger; useful for creating immutable chain, this help to preventing tampering with integrity of already exited entries.

iv) Nodes already in the blockchain network must agree the new block becomes a part of the network and once the consensus made between the nodes the newly generated block can be part of the ledger.

The reminder section of the paper is organized as follows: Section II, introduce the literature review about recent electronic voting mechanisms. In section III, various approaches based on blockchain voting system and measure of few of the frameworks based on blockchain to understand the methodology. Later part discussed about the security concerns and limitation of legal considerations in Section IV. Result discussion obtained in Section V. Finally, conclusion and future work enlisted in Section VI.

2. Literature Review

There are many papers published on the subject of electronic voting system. In this section, we summarize the technique of an electronic voting system.

[1] Introduced the first electronic voting system based on Blind Signature Theorem. The aim of the work was to protect the voter privacy using public key cryptography. Later on, mass research has been done in the topic of electronic voting [2].

Estonia was the first country to implement a voting system back in 2007 in which citizens were able to cast their vote remotely via internet thanks to their electronic national identification card [3].

The ID card used enable authentication and electronic encrypted signature using SHA1/SHA2 [4]. The Estonian ID card also allows access to other Estonian E-services like bank accounts, health insurance and for proof of identity when traveling within the EU. Norway also used an electronic voting system for the country council elections back in 2011 called I-Voting System but the project was later discontinued because of security concerns [5].

Both Estonian and Norwegian electronic systems are criticized of being black boxes, and it’s hard to tell if they respect the voters’ privacy and anonymity. Some research has also been done the applying the zero knowledge proofs and homomorphism encryption in [6].

In [7], the authors proposed interactive Zero-knowledge Proof techniques for voter initialization. In [8] the author proposed a publicly verifiable secret sharing (PVSS) scheme with optimal running time and proposed an election scheme as an application for their PVSS scheme. Other proposals like [9] used the RSA (Rivest-Shamir-Adleman) and factoring assumptions in their voting scheme.

The aim of using the Zero-knowledge proof if to verify the ballot validity without revealing the choice made by the voter. There also exist some proposals to implement voting systems based on Blockchain technology [10].

The main problem of these proposed Blockchain based systems is that they do not protect the voter privacy, although the voter is only known by a public address in the Blockchain network, the committee who issued the right to participate know the corresponding address to each voter, and therefore the voter in not fully anonymous.

The system proposed in this paper uses different components to solve most problems faced when designing and creating an electronic voting system. This work can be used in any scale.
3. Preliminaries of A Blockchain-Based Voting System

Blockchain is now hot topic because of Bitcoin and crypto currency. Though, the technology is so popular now and the use case based on the technology is emerged in recent days. Blockchain based e-voting is essential in order to rectify the issues associated with current various e-voting schemes.

The blockchain based framework basically a distributed nature. All the records are viewed as a transactions’ block will hold all the transactions. With the help of technology a well secure and strong voting system can be implemented. The exploration work outline the idea how the technology useful to implement e-voting system securely.

a. Blockchain

Bitcoin was the first introduced by using blockchain technology. In this all the transactions within public ledger. All the transaction stores in block; after certain number of transaction block eventually becomes completed. Once the process over the block will be added in a network. The chronological order used here for adding new blocks.

“Genesis block or block 0” is the initial block in block chain. The initial block is special block which is hardcoded into the software; which will not contain any reference to a previous block.

After initialization of genesis block “Block 1” is created and once all the transaction of the block completed which is attached to the initial block. Every block contains number of transactions, hash value generated for each block. Merkle root is formed by combining the hash of all the hashes of all the transactions that are part of a block in a blockchain network. Figure 1 is the Merkle root.

![Figure 1. Hash table](image)

The transaction once written inside the block then can’t be modified. To achieve this each block of blockchain maintains the hash value of previous block, changes is not at all possible suppose if any modification needed all the subsequence blocks and the indented block need to modify but practically it’s very difficult task.

Peer to Peer network supports the blockchain design; in peer-to-peer each peer possibly communicate with other peer for exchange the transaction among them. If peer is attached with the current network, it’s fully eligible to sending transaction related communication on the network, this fashion creates decentralized network.

Each node in the network also performs validation and ensures the transaction is valid one. Figure 2 shows the Simplified Bitcoin Block Chain.
b. Current Digital Voting Systems

Digital voting is a new technique around the world. In implementation of digital voting system Estonia is most popular country. National wide ID card given to all Estonian citizens, with the national identity the voters can identified uniquely.

The voting process in this work as follows for voting, the voter needs to enter their card to card reader and once the successful completion of card reader data verification. The voter driven to the web page for that internet available system required.

After login need to enter their OTP and PIN number and verification will be done based on their entered data upon completion of the verification they will be intimated whether the person is eligible for the voting process or not. In case if the verification favors the person he /she can able to cast their vote. The same voting process can be even carried out through any smart phone this is biggest advantage of the work. Through mobile phones voter can login and identify them for voting.

Once the voter cast their vote, the e-votes are passed forwarded to the vote storage server the polled votes are stored in encrypted form until the entire counting process over. All meta data are hidden and the polled voting information written to DVD. Server decrypts transaction information and starts counting finally the results will be displayed. Entire voting process is logged and audited, as seen in Figure 3.

After many reviews researchers found and pointed possible security risks of current digital voting system. One such notable danger is malware on client machine. Malware is any kind of software mainly originated for malfunctioning, there is a possibility for monitor the voter’s activity when the user indented to cast their vote and there is a possible chance for changing the voters vote to different candidate. The other type of risk associated with the current system is attacker, the attacker may try to infect the servers directly through the malware placed on the resultant stored DVD’s. Figure 3 shows the Current Digital System in Estonian.
4. Implementation Of The Model

a. Election Creation
Election ballots created by election administrators using decentralized App (dApp). App will interacts with smart contract created for election, in which administrator list out the candidates and voting district locations.

   This smart contract create smart ballot and those are deployed onto the blockchain, with candidate list, voting district, in each ballot smart contract consider voting district as a one of the parameter. Upon successful creation of election, each node gets permission to interact with other nodes of the network through the smart contracts.

b. Voter Registration
Registration system is developed by the election administrator authorities. Once election is announced the administrators must notify the voters whether they are eligible for voting process.

All eligible voters of the nation need to register for the election using unique identification of the citizen by various documents like Adhar card, Pan Card, Driving License to assert their eligibility. While doing registration user face is captured and it is saved in database for further process. Figure 4 shows the User Registrations

![Figure 4. User Registrations](image)

C. Authentication Phase:
In digital e voting system for casting the vote user need to login in to the system using their credentials. Authentication process as follows all the information entered will be verified, if the information entered is matched with valid voter, the user will be permitted to cast a vote. Authentication process plays vital role in security of the above mentioned system. This will help to ensure someone’s identity isn’t being misused for a fraudulent purpose because in selecting people’s representative every voter’s is important.
For authentication the voter requires three different data; identification number, one time password, ballot card with a QR code. Figure 5 shows the Admin Login.

Figure 5. Admin Login

d. Casting Vote Phase:
Once after successful completion of authentication phase voter will redirected to the voting phase. At the time of registration time the voter face captured by the web camera and stored in a database. Once voter in voting phase the face verification process will be carried out. If the image in database is matched with the captured Image of the voter, then he/she is allowed to cast their Vote. Figure 6 shows the voting phase.

Retracted
On the voting page, all the party whatever party contest in the election symbols /buttons will be there. Voter can cast his /her vote in the election. From the list voters need to choose a candidate and cast their vote. The entire system is designed such a way that it’s very friendly to the user interaction. As soon as voter will fetch their vote, the id of voter logout automatically so we can say that a voter can give only one vote (Auto refresh)

e. Encrypting Votes:
After the successful casting, the application will generate a hash code that contains voter’s unique identification number along with voters’ information and previous block hash value. This method will ensure the uniqueness of each transaction.

f. Adding Block:
Once all the transaction captured and confirmed a new block will be created ad depending on the selection of candidate, the information is recorded in a block. Every block is chained with previous. So changing a transaction is highly impossible for such system.

g. Displaying result:
After the election period is over results will be made available to all the voters on their dashboard by the admin.

5. Limitations
Although the Blockchain technology is very popular but still most of the people not aware about the technology and they fail to understand it completely, due to this will take some more time to emerge and be taken into consideration, which is notable limitation for the technology. Another limitation for the system is a 51% attack is a potential threat to our proposed design

6. Result and Discussion
The evaluation is done on the basis of verification of voters, voting only once per voter, vote converting into blockchain transactions, adding candidates standing for the elections and displaying results after the election is over.
One risk associate with digital e-voting system is voters were forgetting their login credentials like username, password on the day of voting. In such case the voter can’t able to cast their vote because the can’t even enter into the system.

Chance of risk is high some time later on the same day voter try to access the system with correct information or backup authentication services.

Forgotten password can be added to the voter registration website; this will provide pathway for the hackers to attempting to change voter’s password without knowing the concern voter.

A major pitfall of the design majority of mining hash rate theoretically control by someone, leading them to being able to manipulate the public ledger. Need to inverse huge cost for purchase capable hardware. This system tries to exploit voter’s secrecy through their own devices in lots of ways.

7. Conclusion

In exploration research work, a electronic voting system based blockchain technology implemented with smart contracts ensure secure and cost-effective election by promising privacy of voters. Blockchain technology overcome all the limitations and barriers of previous electronic voting systems and ensures secure voting system.

The novel technique enables transparency in elections. Technology used to store data, the system guarantees the public to check and acquire with the decentralized system. But the system is not providing any guaranteed for error free data. blockchain based voting system need to assure that the data fed into it could be error free data.

References

[1] A. Ben Ayed. 2017. A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications (IJNSA) 9(3), (2017), 1–9.
[2] G. Anjan Babau and Dr. M. Padmavathamma. 2006. Optimally efficient multi authority secret Ballot e-election scheme. Journal of Theoretical and Applied Information Technology, 5(2), (2006), 1–4.
[3] Trueb Baltic. 2013. Estonian Electronic ID Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application. (2013). https://www.id.ee/public/TB-SPEC_EstEID-Chip-Appv3_5-20140327.pdf
[4] Ethereum Blog. 2015. On Public and Private Blockchains - Ethereum Blog. (2015). https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
[5] D. Devikanniga, A. Ramu, and A. Haldorai, Efficient Diagnosis of Liver Disease using Support Vector Machine Optimized with Crows Search Algorithm, EAI Endorsed Transactions on Energy Web, p. 164177, Jul. 2018. doi:10.4108/eai.13-7-2018.164177
[6] H. Arandakumar and K. Umamaheswari, Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers, Cluster Computing, vol. 20, no. 2, pp. 1505–1515, Mar. 2017Estonia ID card. [n.d.]. ([n. d.]). https://e-estonia.com/solutions/e-identity/edicard/
[7] D. L. Dill and A.D. Rubin. 2004. E-Voting Security. Security and Privacy Magazine, 2(1) (2004), 22–23.
[8] D. Evans and N. Paul. 2004. Election Security: Perception and Reality. IEEE Privacy Magazine 2(1) (2004), 2–9.
[9] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. 1989. The knowledge complexity of interactive proof systems. SIAM Journal on computing 18, 1 (1989),186–208.